PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

United States Patent and Trademark Office
(Box PCT)
Crystal Plaza 2
Washington, DC 20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 08 January 1999 (08.01.99)	
International application No. PCT/SE98/00897	**Applicant's or agent's file reference** 2988365
International filing date (day/month/year) 14 May 1998 (14.05.98)	**Priority date** (day/month/year) 15 May 1997 (15.05.97)
Applicant SJÖBLOM, Hans	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

08 December 1998 (08.12.98)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer Nicola Wolff
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

Form PCT/IB/331 (July 1992)

2418517

RECORD COPY

PCT
REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty

For receiving Office use only

PCT/SE98/00897

International Application No.

14 -05- 1998

International Filing Date

The Swedish Patent Office
PCT International Application

Name of receiving Office and PCT International Application

Applicant's or agent's file reference
(if desired)(12 characters maximum 2988365

Box No. I TITLE OF INVENTION

ELECTRONIC TRANSACTION

Box No. II APPLICANT

Name and address *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country)*

ACCESS SECURITY SWEDEN AB
Mariebergs Säteri
S-147 92 GRÖDINGE
Sweden

☐ This person is also inventor

Telephone No.

Facsimile No.

Teleprinter No.

State *(i.e. country)* of nationality: Sweden

State *(i.e. country)* of residence: Sweden

This person is applicant for the purposes of : ☐ all designated States ☒ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

Box No. III FURTHER APPLICANT(S) AND/OR /FURTHER INVENTOR(S)

Name and address *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country)*

SJÖBLOM, Hans
Vårgårdsvägen 51
S-133 36 SALTSJÖBADEN
Sweden

This person is

☐ applicant only
☒ applicant and inventor
☐ inventor only *(If this check-box is marked, do not fill in below*

State *(i.e. country)* of nationality: Sweden

State *(i.e. country)* of residence: Sweden

This person is applicant for the purposes of : ☐ all designated States ☐ all designated States except the United States of America ☒ the United States of America only ☐ the States indicated in the Supplemental Box

☐ Further applicants and/or (further) inventors are indicated on a continuation sheet

Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The person identified below is/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as: ☒ agent ☐ common representative

Name and address *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country)*

AWAPATENT AB
P.O. Box 45086
S-104 30 STOCKHOLM
Sweden

Telephone No.
+46 8 440 95 00

Facsimile No.
+46 8 440 95 50

Teleprinter No.
32407 awapat s

☐ Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent

PCT/SE 98/00897

14 -05- 1998

Box No. V DESIGNATION OF STA

The following designations are hereby made under Rule 4.9(a) *(mark the applicable check-boxes; at least one must be marked)*:

Regional Patent

- [x] **AP** **ARIPO Patent**: GH Ghana, GM Gambia, KE Kenya, LS Lesotho, MW Malawi, SD Sudan, SL Sierra Leone, SZ Swaziland, UG Uganda, ZW Zimbabve and any other State which is a Cintracting State of the Harare Protocol and of the PCT
- [x] **EA** **Eurasian Patent:** AM Armenia, AZ Azerbaijan, BY, Belarus, KG Kyrgyzstan, KZ Kazakstan, MD Republic of Moldovia, RU Russian Federation,TJ Tajikistan, TM Turkmenistan and any other States which is a Contracting State of the Eurasian Patent Convention and of the PCT
- [x] **EP** **European Patent**: AT Austria, BE Belgium, CH and LI Switzerland and Liechtenstein, DE Germany, CY Cyprus DK Denmark, ES Spain, FI Finland, FR France, GB United Kingdom, GR Greece, IE Ireland, IT Italy, LU Luxembourg, MC Monaco, NL Netherlands, PT Portugal, SE Sweden, and any other State which is a Contracting State of the European Patent Convention and of the PCT
- [x] **OA** **OAPI Patent**: BF Burkina Faso, BJ Benin, CF Central African Republic, CG Congo, CI Cote d'Ivoire, CM Cameroon, GA Gabon, GN Guinea, ML Mali, MR Mauritania, NE Niger, SN Senegal, TD Chad, TG Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT

(if other kind of protection or treatment desired, specify on dotted line)

National patent *(if other kind of protection or treatment desired, specify on dotted line)*:..

[x] AL	Albania		
[x] AM	Armenia		
[x] AT	Austria	+ Utility Model	
[x] AU	Australia		
[x] AZ	Azerbaijan		
[x] BA	Bosnia and Herzegovina		
[x] BB	Barbados		
[x] BG	Bulgaria		
[x] BR	Brazil		
[x] BY	Belarus		
[x] CA	Canada		
[x] CH/LI	Switzerland and Liechtenstein		
[x] CN	China		
[x] CU	Cuba		
[x] CZ	Czech Republic	+ Utility Model	
[x] DE	Germany	+ Utility Model	
[x] DK	Denmark	+ Utility Model	
[x] EE	Estonia	+ Utility Model	
[x] ES	Spain		
[x] FI	Finland	+ Utility Model	
[x] GB	United Kingdom		
[x] GE	Georgia		
[x] GH	Ghana		
[x] GM	Gambia		
[x] GW	Guinea-Bissau		
[x] HU	Hungary		
[x] ID	Indonesia		
[x] IL	Israel		
[x] IS	Iceland		
[x] JP	Japan		
[x] KE	Kenya		
[x] KG	Kyrgyzstan		
[x] KP	Democratic People's Republic of Korea		
[x] KR	Republic of Korea		
[x] KZ	Kazakstan		
[x] LC	Saint Lucia		
[x] LK	Sri Lanka		
[x] LR	Liberia		
[x] LS	Lesotho		
[x] LT	Lithuania		
[x] LU	Luxembourg		
[x] LV	Latvia		
[x] MD	Republic of Moldova		
[x] MG	Madagascar		
[x] MK	The former Yugoslav Republic of Macedonia		
[x] MN	Mongolia		
[x] MW	Malawi		
[x] MX	Mexico		
[x] NO	Norway		
[x] NZ	New Zealand		
[x] PL	Poland		
[x] PT	Portugal		
[x] RO	Romania		
[x] RU	Russian Federation		
[x] SD	Sudan		
[x] SE	Sweden		
[x] SG	Singapore		
[x] SI	Slovenia		
[x] SK	Slovakia	+ Utility Model	
[x] SL	Sierra Leone		
[x] TJ	Tajikistan		
[x] TM	Turkmenistan		
[x] TR	Turkey		
[x] TT	Trinidad and Tobago		
[x] UA	Ukraine		
[x] UG	Uganda		
[x] US	United States of America		
[x] UZ	Uzbekistan		
[x] VN	Viet Nam		
[x] YU	Yugoslavia		
[x] ZW	Zimbabve		

Check-boxes reserved for designating States (for the purposes of a national patent) which have become party to the PCT after issuance of this sheet:

- [ ]
- [ ]
- [ ]
- [ ]

In addition to the designations made above, the applicant also makes under Rule 4.9(b) all designations which would be permitted under the PCT except the designations of _____

The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit.(*Confirmation of a designation consists of the filing of a notice specifying that designation and the payment of designation and confirmation fees. Confirmation must reach the receiving Office within the 15-month time limit)*

Box No. VI **PRIORITY CLAIM** Further priority claims are indicated in the Supplement Box

The priority of the following earlier application(s) is hereby claimed:

Country *(in which, or for which the application was filed)*	Filing Date *(day,month, year)*	Application No.	Office of filing *(only for regional or international application)*
item (1) Sweden	15 May 1997 15.05.1997	9701814-7	
item (2)			
item (3)			

Mark the following check-box if the certified copy of the earlier application is to be issued by the Office which for the purposes of the present international application is the receiving Office (a fee may be required):

[x] The receiving Office is hereby requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) identified above as item(s): (1) 9701814-7

Box No. VII **INTERNATIONAL SEARCHING AUTHORITY**

Choice of International Searching Authority (ISA) *(If two or more International Authories are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used):* ISA/ SE_____

Earlier search *Fill in where a search (international, international-type or other) by the International Searching Authority has already been carried out or requested and the Authority is now requested to base the international search, to the extent possible, on the results of that earlier search. Identify such search or request either by reference to the relevant application (or the translation thereof) or by reference to the search request:*

Country (or regional Office)	Date (day/month/year)	Number:
Sweden	10 July 1997	SE 97/00775

Box No. VIII **CHECK LIST**

This international Applications contains the following number of sheets:

1.	request	3	sheets ✓
2.	description	15	sheets ✓
3.	claims	5	sheets ✓
4.	abstract	1	sheets ✓
5.	drawings	7	sheets ✓
	Total	31	sheets ✓

This international application is accompanied by the item(s) marked below:

1. [ ] separate signed power of attorney
2. [ ] copy of general power of attorney
3. [ ] statement explaining lack of signature
4. [ ] priority document(s) *identified in Box No. VI as item(s):*
5. [ ] fee calculation sheet
6. [ ] separate indications conerning deposited microorganisms
7. [ ] nucleotide and/or amino acid sequence listing (diskette)
8. [X] other *(specify):* ITS Search Report

Figure No. 3 of the drawings (if any) should accompany the abstract when it is published.

Box No. IX **SIGNATURE OF APPLICANT OR AGENT**

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request)

G. Henningsson

Gunnar Henningsson

For receiving Office use only

1.	Date of actual receipt of the purported international application: 14 -05- 1998		2. Drawing [X] received [ ] not received
3.	Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:		
4.	Date of timely receipt of the required corrections under PCT Article 11(2):		
5.	International Searching Authority specified by the applicant: ISA/ SE	6. [ ] Transmittal of search copy delayed until search fee is paid	

For International Bureau use only

Date of receipt of the record copy by the International Bureau: 19 JUNE 1998 (19.06.98)

PCT/SE 98/00897
14 -05- 1998

ELEKTRONISK TRANSAKTION

Tekniskt område

Föreliggande uppfinning hänför sig allmänt till elektroniska transaktioner, dvs främst betalningar, som sker på elektronisk väg. Uppfinningen avser speciellt elektroniska transaktioner som sker under utnyttjande av ett användarkort, såsom ett bankkort, kreditkort, kontokort, eller dylikt, vilket kort är ett så kallat aktivt kort.

Teknisk bakgrund

Under senare år har intresset för elektroniska transaktioner ökat markant, särskilt i takt med att Internet fått ett kraftigt genomslag. Säkerhetsfrågor har härvid hamnat i fokus, och det har föreslagits olika system och standarder som skall garantera säkerheten i samband med elektroniskt översändande av transaktionsmeddelanden. Av särskilt intresse har varit hur man skall skydda exempelvis över Internet överförda kreditkortsnummer i samband med handel över Internet. Föreslagna system och standarder har det gemensamt att de bygger antingen på att känslig information, som kan missbrukas, t ex ett kreditkortsnummer, icke skall överföras över kommunikationsnätet, eller på att sådan känslig information skall överföras i krypterad form. I båda alternativen ligger tonvikten på förhållandevis komplicerade administrativa rutiner och systemkonfigurationer, etc, vilket såsom inses innebär begränsningar och hinder för ett mera allmänt utnyttjande.

Uppfinningens syfte

Ett huvudsyfte med föreliggande uppfinning är att möjliggöra elektroniska transaktioner på ett förenklat sätt under bibehållande av full säkerhet.

Ett annat syfte är att möjliggöra olika slags elektroniska transaktioner inom ramen för samma grundkoncept.

Ännu ett syfte är att möjliggöra elektroniska transaktioner oberoende av val av kommunikationsväg för utnyttjat transaktionsmeddelande.

Ytterligare ett syfte är att möjliggöra elektroniska transaktioner som i princip icke kräver överföring av utnyttjat transaktionsmeddelande via en säker kommunikationsväg.

Sammanfattning av uppfinningen

Ovannämnda syften uppnås genom de uppfinningssärdrag som framgår av bifogade patentkrav.

Uppfinningen baserar sig sålunda på en insikt om det fördelaktiga i att utnyttja speciella transaktionsmeddelanden, som oberoende och under full egen kontroll skapas av en användare och som har sådan beskaffenhet, att de endast kan ha skapats av användaren i fråga, icke kan ha manipulerats under översändande till en mottagare eller adressat utan att detta lätt kan konstateras (äkthetskontroll), och enkelt kan "valideras" efter översändare i och för slutförande av önskad transaktion. Enligt uppfinningen utnyttjar avsändaren ett honom tillordnat unikt aktivt kort med däri lagrad privat nyckel (vars publika motsvarighet i ett asymmetriskt kryptosystem är allmänt tillgänglig) för att förse ett av avsändaren skapad transaktionsmeddelande med en för avsändaren unik digital signatur, varefter det signerade transaktionsmeddelandet kan översändas på godtyckligt sätt.

Endast en rättmätig användare av det aktiva kortet kan aktivera detta för signering, varigenom ett grundläggande identitetskrav är uppfyllt. Den digitala signaturen innebär vidare ett datalås som omöjliggör meddelandemanipulering utan upptäckt vid senare äkthetskontroll med utnyttjande av den allmänt tillgängliga publika nyckel, som hör till användaren. Användarens oberoende skapande av transaktionsmeddelandet innebär full kontroll av innehållet i meddelandet. Uppfinningen innebär sålunda krav på koppling av känsliga uppgifter, såsom ett kortnummer, i det överförda transaktionsmeddelandet till en digital

signatur för att uppgifterna i fråga skall vara användbara. I avsaknad av en koppling till en digital signatur är uppgifterna sålunda i princip värdelösa och kan följaktligen icke missbrukas för falska nättransaktioner, även om det skulle kunna fångas upp av någon utomstående i samband med ett översändande av transaktionsmeddelandet. Hur översändandet sker blir i princip utan betydelse. Detta innebär ett synsätt som är helt motsatt dagens strävanden efter att åstadkomma särskilda, säkra, dvs krypterade, kommunikationssystem för översändande av transaktionsmeddelanden över exempelvis Internet.

Det är föredraget att ett transaktionsmeddelande enligt uppfinningen innehåller uppgift om avsändare, transaktionsbelopp och mottagare samt företrädesvis en föränderlig uppgift, såsom ett löpnummer.

Enligt uppfinningen skapar sålunda användaren vad som kan sägas vara en signerad "elektronisk check", vilken kan översändas på godtyckligt sätt och vid godtycklig tidpunkt till en adressat eller mottagare.

Efter mottagning kan ett transaktionsmeddelande enligt uppfinningen kontrolleras vad gäller äkthet genom kontroll av den digitala signaturen, varefter "validering" och gottskrivning eller kreditering av mottagaren med transaktionsbeloppet ifråga kan ske på godtyckligt lämpligt sätt, lämpligen enligt samma principer som gäller för inlösen av en vanlig check eller för clearing i samband med kortköp.

Enligt uppfinningen kan det översända, signerade transaktionsmeddelandet innehålla erforderliga transaktionsuppgifter i klartext, varvid den digitala signaturen på känt sätt kan vara beräknad på ett kondensat av meddelandeuppgifterna. Detta innebär att senare äkthetskontroll, validering och kreditering på mottagarsidan underlättas, eftersom erforderliga uppgifter direkt föreligger, såsom uppgift om avsändare, som gör det enkelt att hämta rätt publik nyckel i och för äkthetskontroll av den digitala signaturen.

Om den digitala signaturen utförs på hela transaktionsmeddelandet, så att detta överförs i krypterad form, kan det överförda transaktionsmeddelandet vara försett med särskild avsändaruppgift som gör det möjligt att på mottagarsidan hämta rätt publik nyckel för äkthetskontrollen och omvandling av transaktionsmeddelandet till klartext.

Enligt uppfinningen kan transaktionsmeddelandet innehålla avsändaruppgift av godtyckligt lämpligt slag, såsom åtminstone en av följande uppgifter: ett kortnummer, ett bankkortnummer, ett betalkortnummer, ett kreditkortnummer, ett kontonummer, ett fakturanummer och ett ID-nummer. Om det enligt uppfinningen utnyttjade aktiva kortet är ett till ett konto kopplat kort, såsom ett kreditkort, kan det vara föredraget att såsom avsändaruppgift utnyttja tillhörande kortnummer. Såsom fackmannen inser är det dock möjligt att använda varje slags uppgift, som på mottagarsidan enkelt kan kopplas ihop med en användaridentitet och därigenom med ett tillhörande konto, som skall debiteras.

För mottagaruppgiften gäller i princip samma sak. Exempelvis kan det vara fråga om åtminstone en av följande uppgifter: ett kortnummer, ett bankkortnummer, ett betalkortnummer, ett kreditkortnummer, ett kontonummer, ett fakturanummer och ett ID-nummer. Även här är det tillräckligt att ifrågavarande uppgift på mottagarsidan entydigt kan relateras till en betalningsmottagare. Det skall påpekas att överförande av ett transaktionsbelopp till en mottagare inte behöver innebära att ett mottagarkonto krediteras, utan att det också kan vara fråga om att exempelvis en administrativ enhet, som mottager transaktionsmeddelandet, efter äkthetskontroll och validering debiterar ett avsändarkonto och till mottagaren sänder vad som kan betraktas som en check eller postanvisning.

Såsom tidigare redovisats är ett väsentligt särdrag hos föreliggande uppfinning att avsändaren, dvs användaren av det aktiva kortet, skapar och signerar transak-

tionsmeddelandet under egen kontroll, dvs i princip oberoende av uppkoppling mot ett kommunikationsnät och av en datadialog med en mottagare, ehuru en dylik dialog naturligtvis kan förekomma i samband med översändande av ett signerat transaktionsmeddelande. Transaktionsmeddelandet skapas följaktligen företrädesvis fristående från kommunikationsnätet eller off-line. Detta innebär att avsändaren har full kontroll över vilka uppgifter som inmatas för skapande av transaktionsmeddelandet. Signeringen kan såsom inses endast åstadkommas av avsändaren, eftersom denne i normalfallet är ensam om att kunna aktivera sitt aktiva kort och utlösa signeringen. När det gäller översändandet eller överlämnandet av det signerade transaktionsmeddelandet finns dock icke några restriktioner, såsom utan vidare inses. Exempelvis kan användaren eller någon denne behjälplig person ta med sig det aktiva kortet med det däri befintliga, signerade transaktionsmeddelandet för senare meddelandeavsändande, för meddelandeavsändande på annan plats, etc, dvs stor valfrihet råder. Det signerade transaktionsmeddelandet skulle också kunna föras över på ett särskilt mellanlagrings- eller transportmedium i och för överföring till en mottagare och/eller adressat.

Enligt uppfinningen är det fördelaktigt att transaktionsmeddelandet skapas i det aktiva kortet. Transaktionsmeddelandet kan härvid lämpligen skapas med hjälp av i det aktiva kortet i förväg inlagd programvara och företrädesvis i kortet i förväg inlagd avsändaruppgift, t ex ett kortnummer. Lämpligen skapas också automatiskt ett nytt löpnummer för varje transaktionsmeddelande. Inmatning av erforderliga meddelandeuppgifter i kortet kan ske på olika sätt, t ex medelst på det aktiva kortet anordnade inmatningsorgan, varvid kortet med fördel utgörs av ett så kallat avancerat aktivt kort. För transaktionsmeddelandet erforderliga uppgifter kan också inmatas medelst en skyddad kortterminal, som med fördel kan utgöras av användarens egen kortläsarförsedda terminal eller da-

tor. För transaktionsmeddelandet erforderliga uppgifter kan också inmatas medelst en separat kortkommunikationsenhet, varvid den senare företrädesvis senare även fungerar såsom kortaktivator. En dylik enhet kan med fördel vara utförd som en liten, bärbar enhet, som användaren kan ha med sig och som av användaren utnyttjas då han vill aktivera sitt kort och/eller inmata uppgifter i kortet i en miljö, där någon skyddad kortterminal inte finns.

För transaktionsmeddelandet erforderliga uppgifter kan också inmatas medelst en av det aktiva kortet styrd telekommunikationsenhet, speciellt en mobil sådan, såsom en mobiltelefonanordning. I detta sammanhang kan enheten också utnyttjas för översändande av det signerade transaktionsmeddelandet, t ex med utnyttjande av en tjänst av så kallad SMS-typ.

Fackmannen inser att det även är möjligt att skapa själva transaktionsmeddelandet utanför det aktiva kortet exempelvis vid utnyttjande av något av ovannämnda uppgiftsinmatningsorgan. Det skapade transaktionsmeddelandet inmatas därefter i det aktiva kortet i och för signering.

Enligt en första aspekt på föreliggande uppfinning åstadkommes ett förfarande för genomförande av elektroniska transaktioner, varvid en avsändare av transaktionsmeddelanden tilldelas ett aktivt kort med tillhörande unik identitet och i kortet skyddat lagrad privat nyckel och varvid en tillhörande publik nyckel hålls allmänt tillgänglig, vilket förfarande utmärks av att avsändaren i samband med en elektronisk transaktion under egen kontroll, företrädesvis genom egen inmatning av meddelandeuppgifter, skapar ett transaktionsmeddelande, som innehåller för transaktionen erforderliga uppgifter, samt i sitt aktiva kort förser det skapade transaktionsmeddelandet med sin digitala signatur under utnyttjande av sin privata nyckel i och för senare utmatning och avsändande av transaktionsmeddelandet.

Enligt en andra aspekt på föreliggande uppfinning åstadkommes ett aktivt kort för genomförande av elektroniska transaktioner, vilket kort innefattar organ för lagring av kortidentifieringsuppgifter, organ för skyddad lagring av en privat nyckel, organ för lagring av en asymmetrisk algoritm, organ för inmatning av transaktionsuppgifter i kortet, processororgan för att i kortet skapa ett transaktionsmeddelande baserat på inmatade transaktionsuppgifter, såsom uppgifter som belopp och mottagare, och eventuellt i kortet lagrade uppgifter såsom uppgifter om avsändare och företrädesvis ett löpnummer, och för att förse transaktionsmeddelandet med en digital signatur på basis av nämnda privata nyckel och nämnda asymmetriska algoritm, samt organ för utmatning av det signerade transaktionsmeddelandet.

Enligt en tredje aspekt på föreliggande uppfinning åstadkommes en kombination av ett aktivt kort och en för kommunikation med det aktiva kortet anordnad användarkontrollerad kommunikationsenhet, med vilken kortet är anordnat att sammanföras i och för åstadkommande av ett elektroniskt transaktionsmeddelande, varvid kortet innefattar organ för skyddad lagring av en privat nyckel, organ för lagring av en asymmetrisk algoritm, och processororgan för att förse ett skapat transaktionsmeddelande med en digital signatur baserad på nämnda privata nyckel och nämnda algoritm, och varvid kommunikationsenheten innefattar organ för inmatning av transaktionsuppgifter, varjämte organ är anordnade i kommunikationsenheten och/eller i kortet för att skapa nämnda transaktionsmeddelande.

En fjärde aspekt på föreliggande uppfinning innebär användning av ett aktivt kort med däri lagrad privat nyckel och asymmetrisk kryptoalgoritm för kommunikationsnätoberoende åstadkommande i kortet av ett elektroniskt transaktionsmeddelande försett med en på den privata nyckeln baserad digital signatur.

Ytterligare aspekter på särdrag hos uppfinningen kommer att framgå av följande närmare beskrivning av olika utföringsexempel under hänvisning till bifogade ritningar.

Kort beskrivning av ritningarna

Fig. 1 är en schematisk illustration av ett exempel på genomförande av elektroniska transaktioner, under utnyttjande av ett öppet nät, såsom Internet, i enlighet med en uföringsform av föreliggande uppfinning.

Fig. 2 är en schematisk illustration av samma slag som i Fig. 1 exemplifierande alternativa genomföranden av elektroniska transaktioner i enlighet med uppfinningen.

Fig. 3 är en schematisk illustration av ett exempel på genomförande av elektroniska transaktioner, under utyttjande av en butikskortterminal, i enlighet med en anan utföringsform av föreliggande uppfinning.

Fig. 4 är en schematisk illustration av samma slag som i Fig. 3 med ett annat exempel på genomförande av elektroniska transaktioner, under utnyttjande av en butikskortterminal, i enlighet med föreliggande uppfinning.

Fig. 5 är en schematisk illustration av ett exempel på genomförande av elektroniska transaktioner, under utnyttjande av mobil telefoni, i enlighet med ännu en utföringsform av föreliggande uppfinning.

Fig. 6 är en schematisk illustration av ett exempel på genomförande av elektroniska transaktioner, under utnyttjande av ett öppet nät för direkt kontakt med en bank, i enlighet med ytterligare en utföringsform av föreliggande uppfinning.

Fig. 7 är en schematisk illustration av exempel på hur ett avancerat aktivt kort kan utnyttjas för genomförande av elektroniska transaktioner i enlighet med föreliggande uppfinning.

Beskrivning av utföringsformer

I Fig. 1 illustreras schematiskt en första utföringsform av uppfinningen, vilken kan användas för kreditkortsbetalning över ett öppet nät, såsom Internet,

mellan en avsändare och en mottagare ingående i ett nätverk. Avsändaren förfogar över ett aktivt kort 1 och en med lämplig kortläsare (antydd vid 2) försedd dator 3, vilken typiskt kan vara en hemdator och vilken har anslutning till Internet 5. En nätverksserver 7 är ansluten till nätet 5 samt till i nätverket ingående, olika kreditkortsadministratörer 8 och 9. De senare är på konventionellt sätt anslutna till varandra och till olika kontoförande institutioner, såsom banker 10, 11. I föreliggande exempel antas avsändaren ha konto i banken 10 och ett kreditkort administrerat av administratören 8, under det att mottagaren 12 har konto i banken 11 och ett kreditkort administrerat av administratören 9.

En tillförlitlig tredje part (TTP) 13 är nätverksadministratör och ansvarar för erforderlig nyckelhantering. TTP 13 tilldelar sålunda respektive användare hans privata nyckel, som finns skyddat lagrad i användarens kort 1, samt håller en katalog 15 tillgänglig, från vilken respektive användares publika nyckel kan hämtas.

Användarens aktiva kort 1, som även har konventionell kreditkortsfunktion, innehåller på känt sätt minnes- och processororgan i form av en eller flera integrerade kretsar (antydda vid 17), liksom konventionella organ för att möjliggöra kommunikation mellan kortet och en kortläsare, då kortet är placerat i den senare.

Utöver den tidigare nämnda privata nyckeln innehåller nämnda minne- och processororgan en kryptoalgoritm av asymmetrisk typ, vilken kan vara en DES-algoritm, och programvara för genomförande av signering av ett transaktionsmeddelande baserat på den privata nyckeln och nämnda kryptoalgoritm. Det aktiva kortet 1 aktiveras på godtyckligt lämpligt sätt, t ex medelst i kortet inmatat PIN eller biometriskt.

Vid genomförande av en transaktion placeras kortet 1 i datorns 3 kortläsare 17 och kortet aktiveras, om så icke skett dessförinnan. Skapandet av ett transaktionsmeddelande kan nu ske i det aktiva kortet 1 och/eller i

datorn 3. Om skapandet sker uteslutande i kortet, vilket ur säkerhetssynpunkt kan vara att föredraga, innehåller kortet också härför lämplig programvara. I detta fall inmatas erforderliga uppgifter för transaktionsmeddelandet (speciellt om belopp och mottagare) via datorns 3 tangentbord in i kortet.

Om själva transaktionsmeddelandet skapas i datorn, har denna försetts med härför erforderlig programvara, som lämpligen levererats till användaren i samband med utgivandet av det aktiva kortet. Inmatning av meddelandeuppgifter sker även här via tangentbordet.

Det är fördelaktigt att som avsändaruppgift använda en kortidentifikation, såsom det aktiva kortets nummer, som ges automatiskt av kortet i samband med skapandet av transaktionsmeddelandet. Som mottagaruppgift kan med fördel inmatas mottagarens kortnummer.

Efter skapandet av transaktionsmeddelandet skall detta förses med ett löpnummer och signeras, vilket såsom nämnts sker i kortet. Om själva meddelandet skapats i kortet kan det för att begränsa den programvara, som måste finnas i kortet, vara önskvärt att utföra den digitala signaturen på själva meddelandet, varvid meddelandet får formen av kryptotext. Det därefter översända signerade meddelandet måste då kunna ge information om avsändaren, så att för äkthetskontroll erforderlig publik nyckel kan inhämtas, såsom kommer att redovisas senare. Speciellt om transaktionsmeddelandet skapas i en skyddad egen dator, kan det vara lämpligt att generera den digitala signaturen på ett kondēnsat av själva meddelandet, varvid detta senare kommer att föreligga i klartext och också kan översändas i klartext.

Det signerade transaktionsmeddelandet kan nu med fördel ges formen av E-post och därefter sändas över nätet 5 till nätverksservern 7.

Om transaktionsmeddelandet är i klartext, kan servern 7 baserat på uppgifterna i transaktionsmeddelandet utan vidare sända det signare meddelandet antingen till

avsändarens eller mottagarens kortadministratör 8 respektive 9 i och för äkthetskontroll samt, om äkthet konstateras, efterföljande validering, debitering av avsändaren och kreditering av avsändaren av ifrågavarande transaktionsbelopp, under utnyttjande av lämplig clearingprocedur.

Äkthetskontrollen innebär att exempelvis avsändarens kortadministratör inhämtar avsändarens publika nyckel från en egen nyckelkatalog eller katalogen 15 hos TTP 13 och med hjälp därav och av ifrågavarande kryptoalgoritm kontrollerar meddelandets digitala signatur.

Om det av servern mottagna meddelandet inte är i klartext, inhämtar servern 7 från katalogen 15 den publika nyckel som hör till den avsändare som kan identifieras av det mottagna, signerade transaktionsmeddelandet, t ex på basis av en särskild avsändaruppgift, såsom en nätverksidentitet eller Internet-identitet. Efter konventionell dekryptering av meddelandet med utnyttjande av den inhämtade publika nyckeln har servern 7 tillgång till meddelandets uppgifter i klartext och kan skicka meddelandet vidare, i och för äkthetskontroll etc, såsom nämnts ovan.

Ännu ett alternativ här är att det på nätet 5 utsända meddelandet förses med en angiven address till behörig kortadministratör, t ex 8, så att servern 7 kan direkt dirigera meddelandet dit för fortsatt behandling enlig ovan. Om det signerade meddelandet icke är i klartext, måste även här det mottagna meddelandet ge sådan information att rätt publik nyckel kan inhämtas i och för äkthetskontroll och dekryptering av själva meddelandet.

I Fig. 2 illustreras schematiskt en andra utföringsform av uppfinningen, som utnyttjar i grunden samma konfiguration som i Fig. 1, ehuru transaktionsmeddelandet från avsändaren sänds direkt till en mottagares dator 21 via nätet 5. Mottagaren sänder meddelandet vidare, vilket kan ske via nätet till servern 7, såsom antytts med pilen 23, eller via någon annan väg, som antyds via pilen 25.

I denna utföringsform kan det vara lämpligt att själva meddelandet är i klartext, så att mottagaren kan se uppgifterna däri, även om han inte har omedelbar tillgång till avsändarens publika nyckel i och för äkthetskontroll eller dekryptering av den digitala signaturen. Det signerade meddelandet kan emellertid av avsändaren vid behov krypteras med en mottagaren tillhörig publik nyckel, varvid mottagaren vid mottagandet dekrypterar meddelandet med utnyttjande av sin egen privata nyckel och tillhörande kryptoalgoritm och därefter vidarebefordrar det dekrypterade men alltjämt signerade meddelandet.

I fallet med en annan transportväg 25 än nätet 5 kan det vara fördelaktigt att utnyttja ett mellanlagringsmedium, t ex en diskett (antydd vid 26), som mottagaren på lämpligt och säkert sätt överlämnar till sin kortadministratör eller bank för fortsatt behandling i enlighet med vad som beskrivits ovan. Det inses att mottagaren kan samla ett antal mottagna transaktionsmeddelanden på ett dylikt mellanlagringsmedium, innan åtgärder för den fortsatta behandlingen vidtages.

I Fig. 3 illustreras schematiskt en utföringsform av uppfinningen som lämpar sig för transaktioner via en främmande "terminal" 31 och som utnyttjar en användarkontrollerad portabel enhet 33 för skapande av ett transaktionsmeddelande.

Enheten 33 utgörs av en kombinerad aktivator och uppgiftsinmatare för det aktiva kortet. Enheten 33 är på lämpligt sätt anordnad för kommunikation med kortet 1, t ex genom att den inbegriper en integrerad kortläsare, i vilket kortet förs in. Enheten 33 har vidare en tangentuppsättning och en display.

Vid betalning exempelvis i en butik placeras kortet i enheten 33 och aktiveras t ex genom att en PIN-kod inmatas medelst enhetens tangentuppsättning. Medelst tangentuppsättningen inmatas dessutom erforderliga betalningsuppgifter, såsom belopp och mottagare. Om transaktionsmeddelandet både skapas och signeras i själva kor-

tet, överförs själva uppgifterna till kortet. Om själva meddelandet och eventuellt ett kondensat därav skall skapas i enheten 33, i och för överföring till och signering i kortet 1, är enheten försedd med processororgan och erforderlig programvara härför.

Kortet med det signerade transaktionsmeddelandet avlägsnas nu från enheten 33 och införs i butikens läsare/terminal 31, varifrån meddelandet sänds för fortsatt behandling på samma sätt som redovisats tidigare. Godkänd äkthetskontroll och validering kan lämpligen innebära att en kvittens sänds tillbaka till terminalen.

Det inses att terminalen 31 naturligtvis skulle kunna kommunicera med servern 7 på annat sätt än via nätet 5, t ex via en skyddad förbindelse.

I Fig. 4 illustreras en variant av den utföringsform som visas i Fig. 3. Enheten 33 i Fig. 3 är härvid utbytt mot en skyddad, företrädesvis fristående dator eller terminal 43, som kan vara uppställd i exempelvis en butik och möjliggör fristående, säkert skapande av ett transaktionsmeddelande på likartat sätt som beskrivits i anslutning till Fig. 3, i och för inmatning i en butikskortterminal 31.

I Fig. 5 illustreras en utföringsform av föreliggande uppfinning som innebär utnyttjande av en mobiltelefonanordning 51 och ett tillhörande mobiltelenät 55. Mobiltelefonanordningen inbegriper utöver en mobiltelefonfunktion även sådan aktivering- och inmatningsfunktion som beskrivits i samband med enheten 33 i Fig. 3. Mobiltelefonfunktionen är företrädesvis också styrd av det aktiva kortet.

Medelst telefonfunktionen översändes det signerade transaktionsmeddelandet till en enhet eller central 57, som ombesörjer fortsatt behandling av transaktionsmeddelandet exempelvis i enlighet med vad som beskrivits i anslutning till föregående figurer.

Översändandet av transaktionsmeddelandet kan med fördel ske under utnyttjande av en så kallad SMS-tjänst eller liknande hos mobiltelenätet.

Enheten 57 skulle också kunna vara en särskild central, som efter äkthetskontroll etc. ombesörjer betalningar baserat på mottagna transaktionsmeddelanden.

I Fig. 6 illustreras en utföringsform av föreliggande uppfinning som med fördel kan utnyttjas för ombesörjande av betalningsuppdrag. Hos en avsändare, dvs betalare, skapas signerade transaktionsmeddelanden såsom beskrivits, här exemplifierat med samma metod som i Fig. 1. Transaktionsmeddelandet sänds till avsändarens kontoförande bank 10, som i en katalog 60 har tillgång till avsändarens publika nyckel. Det inses att banken skulle kunna vara kortutfärdare och nyckeladministratör och att avsändaruppgiften i transaktionsmeddelandet lämpligen kan utgöras av avsändarens bankkontonummer.

Efter mottagande av ett transaktionsmeddelande och äkthetskontroll därav ombesörjer avsändarens bank 10 genom en clearingprocedur att den i transaktionsmeddelandet lämpligen genom tillhörande bankkontonummer identifierade betalningsmottagaren gottskrivs ifrågavarande belopp, dvs att mottagarens konto i mottagarens bank 11 krediteras beloppet ifråga.

Ett annan alternativ möjlighet är att avsändarens bank 10 sänder en utbetalningsavi direkt till mottagaren 12 exempelvis baserat på mottagaruppgifter i transaktionsmeddelandet. Detta alternativ är antytt medelst den streckade linjen 62 i Fig. 6.

I utförandet enligt Fig. 6 kan det för ökande av säkerheten vara lämpligt att kryptera det översända signerade transaktionsmeddelandet. Avsändaren använder då bankens 10 publika nyckel och företrädesvis samma kryptoalgoritm, som utnyttjas för signeringen. Banken 10 kan såsom inses utan vidare utföra dekryptering med utnyttjande av sin privata nyckel.

Om banken 10 är administratör av avsändarens nyckelpar, dvs besitter såväl den publika nyckel som den privata nyckel som hör till avsändaren, kan avsändaren alternativt utföra krypteringen av det signerade meddelandet med sin publika nyckel. Banken 10 kan då dekryptera det översända meddelandet med utnyttjande av avsändarens privata nyckel, som hämtas från en katalog, innan äkthetskontroll genomförs med utnyttjande av avsändarens publika nyckel.

I Fig. 7 illustreras slutligen schematiskt användning av ett så kallat avancerat aktivt kort i samband med uppfinningen. Det avancerade aktiva kortet 71 har även en tangentuppsättning och en display, som medger att ett signerat transaktionsmeddelande kan skapas i kortet helt och hållet utan externa hjälpmedel. Kortet kan därefter införas i exempelvis en dator eller en terminal i och för vidaresändning av meddelandet och fortsatt behandling i enlighet med vad som beskrivits tidigare.

Ehuru uppfinningen illustrerats genom ett antal utföringsexempel, är uppfinningen självfallet icke inskränkt därtill, utan ändringar och modifikationer är möjliga inom ramen för efterföljande patentkrav. Sålunda kan enskilda särdrag från de olika utföringsexemplen sammanföras i nya kombinationer inom ramen för uppfinningstanken.

PATENTKRAV

1. Förfarande vid genomförande av elektroniska transaktioner, varvid en avsändare av transaktionsmeddelanden tilldelas ett aktivt kort med tillhörande unik identitet och i kortet skyddat lagrad privat nyckel och varvid en tillhörande publik nyckel hålls allmänt tillgänglig, k ä n n e t e c k n a t av att avsändaren i samband med en elektronisk transaktion under egen kontroll, företrädesvis genom egen inmatning av meddelandeuppgifter, skapar ett transaktionsmeddelande, som innehåller för transaktionen erforderliga uppgifter, samt i sitt aktiva kort förser det skapade transaktionsmeddelandet med sin digitala signatur under utnyttjande av sin nämnda privata nyckel i och för senare utmatning och avsändande av transaktionsmeddelandet.

2. Förfarande enligt krav 1, k ä n n e t e c k n a t av att i transaktionsmeddelandet ingår uppgifter om avsändare, mottagare, belopp och företrädesvis ett transaktionslöpnummer.

3. Förfarande enligt krav 1 eller 2, k ä n n e t e c k n a t av att transaktionsmeddelandet skapas fristående från det kommunikationsnät, som utnyttjas för senare avsändande av transaktionsmeddelandet.

4. Förfarande enligt krav 3, k ä n n e t e c k n a t av att transaktionsmeddelandet skapas off-line.

5. Förfarande enligt något av föregående krav, k ä n n e t e c k n a t av att transaktionsmeddelandet skapas i det aktiva kortet.

6. Förfarande enligt krav 5, k ä n n e t e c k n a t av att transaktionsmeddelandet skapas med hjälp av i det aktiva kortet i förväg inlagd programvara och företrädesvis även i kortet i förväg inlagda avsändaruppgifter.

7. Förfarande enligt krav 5 eller 6, k ä n n e t e c k n a t av att för transaktionsmeddelandet erforderliga uppgifter inmatas medelst på det aktiva kortet

anordnade inmatningsorgan, varvid kortet företrädesvis är ett så kallat avancerat aktivt kort.

8. Förfarande enligt något av kraven 1-6, k ä n n e t e c k n a t av att för transaktionsmeddelandet erforderliga uppgifter inmatas medelst en skyddad kortterminal.

9. Förfarande enligt något av kraven 1-6, k ä n n e t e c k n a t av att för transaktionsmeddelandet erforderliga uppgifter inmatas medelst en separat kortkommunikationsenhet, varvid den senare företrädesvis även är en kortaktivator.

10. Förfarande enligt något av kraven 1-6, k ä n n e t e c k n a t av att för transaktionsmeddelandet erforderliga uppgifter inmatas medelst en av det aktiva kortet styrd telekommunikationsenhet, speciellt en mobil sådan, såsom en mobiltelefon.

11. Förfarande enligt något av föregående krav, k ä n n e t e c k n a t av att transaktionsmeddelandet innehåller avsändaruppgift i form av åtminstone en av följande uppgifter: ett kortnummer, ett bankkortnummer, ett betalkortnummer, ett kreditkortnummer, ett kontonummer, ett fakturanummer, och ett ID-nummer.

12. Förfarande enligt något av föregående krav, k ä n n e t e c k n a t av att transaktionsmeddelandet innehåller mottagaruppgift i form av åtminstone en av följande uppgifter: ett kortnummer, ett bankkortnummer, ett betalkortnummer, ett kreditkortnummer, ett kontonummer, ett fakturanummer och ett ID-nummer.

13. Förfarande enligt något av föregående krav, k ä n n e t e c k n a t av att det signerade transaktionsmeddelandet sänds till en kort- eller kontoadministratör avseende avsändaren eller mottagaren, att äkthetskontroll av transaktionsmeddelandets digitala signatur sker med utnyttjande av den publika nyckel, som är tilldelad den som av det överförda transaktionsmeddelandet identifieras såsom avsändare, och att mottagaren om äkthet föreligger

gottskrivs transaktionsbeloppet genom en clearing-process.

14. Förfarande enligt krav 13, k ä n n e t e c k n a t av att det signerade transaktionsmeddelandet först sänds till mottagaren vilken eventuellt efter egen kontroll av meddelandets digitala signatur vidarebefordrar det signerade transaktionsmeddelandet till nämnda kort- eller kontoadministratör.

15. Förfarande enligt något av kraven 1-12, k ä n n e t e c k n a t av att det signerade transaktionsmeddelandet krypteras med utnyttjande av en publik nyckel tillhörande den adressat, vartill transaktionsmeddelandet sänds, att det krypterade signerade transaktionsmeddelandet sänds till adressaten, att adressaten med utnyttjande av sin privata nyckel dekrypterar det signerade transaktionsmeddelandet, att äkthetskontroll av transaktionsmeddelandets digitala signatur sker med utnyttjande av den publika nyckel, som är tilldelad den som av det överförda transaktionsmeddelandet identifieras såsom avsändare, och att mottagaren om äkthet föreligger gottskrivs transaktionsbeloppet genom en clearingprocess.

16. Förfarande enligt krav 15, k ä n n e t e c k n a t av att adressaten är mottagaren, att mottagaren efter dekrypteringen sänder det signerade transaktionsmeddelandet till en kort- eller kontoadministratör, varefter nämnda äkthetskontroll sker.

17. Förfarande enligt något at kraven 1-12, k ä n n e t e c-k n a t av att det signerade transaktionsmeddelandet krypteras med utnyttjande av avsändarens publika nyckel samt förses med avsändaruppgift och därefter sänds till en kort- eller kontoadministratör, som har avsändarens privata nyckel och som företrädesvis är utfärdare av användarens aktiva kort, att nämnda administratör dekrypterar det mottagna krypterade meddelandet med utnyttjande av nämnda privata nyckel, att äkthetskontroll av det dekrypterade transaktionsmeddelandets digitala signatur sker med utnyttjande av den publika nyckel, som

är tilldelad den som av det överförda transaktionsmeddelandet identifieras såsom avsändare, och att mottagaren om äkthet föreligger gottskrivs transaktionsbeloppet genom en clearingprocess.

18. Förfarande enligt något av kraven 1-14, k ä n n e t e c k n a t av att det signerade transaktionsmeddelandet sänds okrypterat, speciellt via ett allmänt kommunikationsnät, såsom Internet eller telekommunikationsnät.

19. Förfarande enligt något av föregående krav, k ä n n e t e c k n a t av att det signerade transaktionsmeddelandet sänds såsom E-post.

20. Förfarande enligt något av kraven 1-18, k ä n n e t e c k n a t av att det signerade transaktionsmeddelandet sänds via ett mobiltelefoninät, speciellt med utnyttjande av så kallad SMS-tjänst.

21. Aktivt kort för genomförande av elektroniska transaktioner, innefattande organ för lagring av kortidentifieringsuppgifter, organ för skyddad lagring av en privat nyckel, organ för lagring av en asymmetrisk algoritm, organ för inmatning av transaktionsuppgifter i kortet, processororgan för att i kortet skapa ett transaktionsmeddelande baserat på inmatade transkationsuppgifter, såsom uppgifter om belopp och mottagare, och eventuellt i kortet lagrade uppgifter såsom uppgifter om avsändare och företrädesvis ett löpnummer, och för att förse transaktionsmeddelandet med en digital signatur på basis av nämnda privata nyckel och nämnda asymmetriska algoritm, samt organ för utmatning av det signerade transaktionsmeddelandet.

22. Kort enligt krav 21, k ä n n e t e c k n a t av att det är av så kallad avancerad typ.

23. Kombination av ett aktivt kort och en för kommunikation med det aktiva kortet anordad användarkontrollerad kommunikationsenhet, med vilken kortet är anordnat att sammanföras i och för åstadkommande av ett elektroniskt transaktionsmeddelande, varvid kortet innefattar

organ för skyddad lagring av en privat nyckel, organ för lagring av en asymmetrisk algoritm, och processororgan för att förse ett skapat transaktionsmeddelande med en digital signatur baserat på nämnda privata nyckel och nämnda algoritm, och varvid kommunikationsenheten innefattar organ för inmatning av transaktionsuppgifter, varjämte organ är anordnade i kommunikationsenheten och/eller i kortet för att skapa nämnda transaktionsmeddelande.

24. Kombination enligt krav 23, k ä n n e t e c k n a t av att kommunikationsenheten är en mobil telekommunikationsanordning.

25. Kombination enligt krav 23, k ä n n e t e c k n a t av att kommunikationsenheten är en kombinerad kortaktivator och uppgiftsinmatare/behandlare.

26. Användning av ett aktivt kort med däri lagrad privat nyckel för kommunikationsnätoberoende åstadkommande av ett elektroniskt transaktionsmeddelande försett med en på den privata nyckeln baserad digital signatur.

SAMMANDRAG

Förfarande och anordning för genomförande av elektroniska transaktioner. En avsändare skapar under full egen kontroll ett transaktionsmeddelande i ett aktivt kort (1) och förser meddelandet med sin digitala signatur i kortet i och för senare utmatning och avsändande.

(Fig. 1)

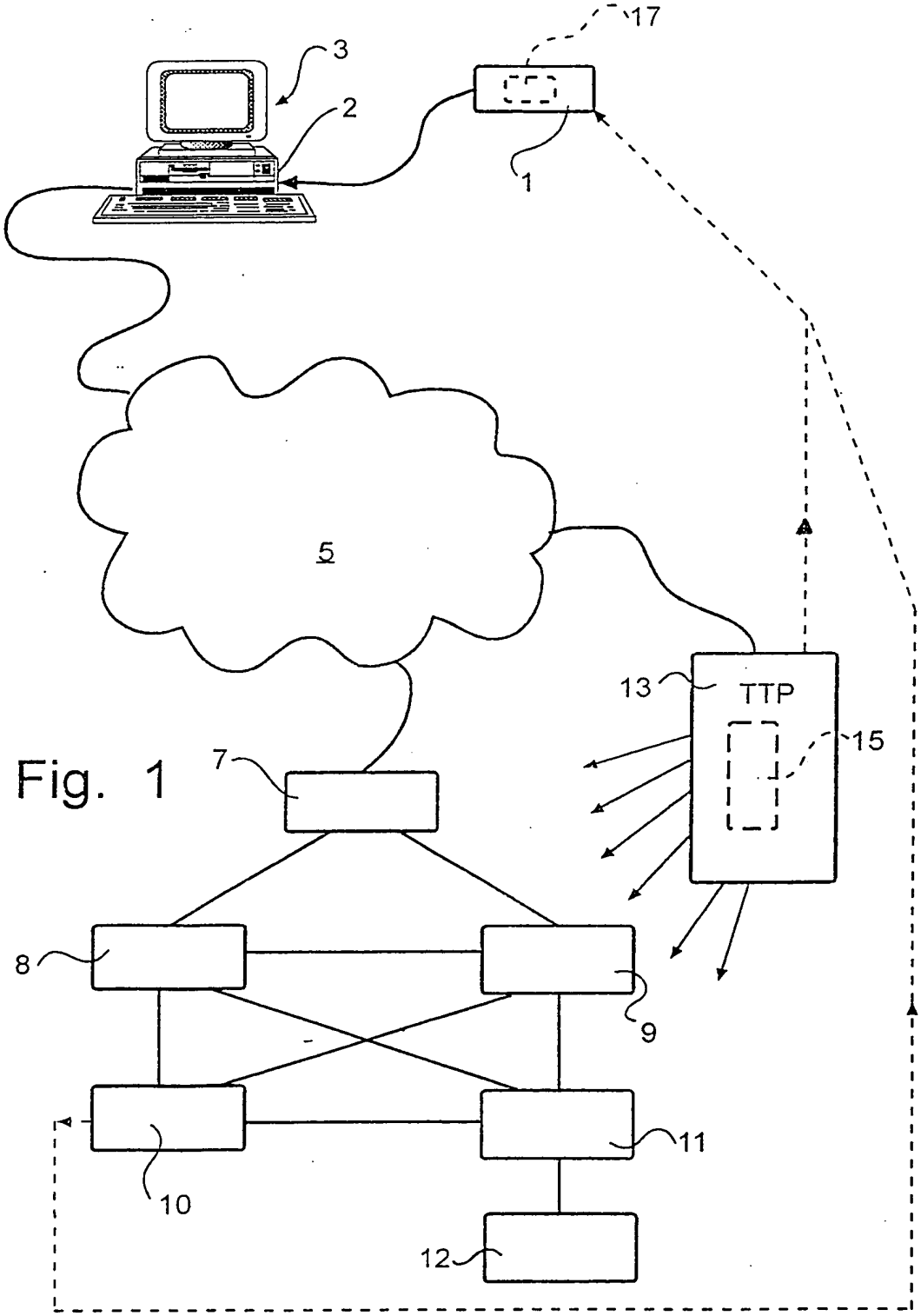


Fig. 1

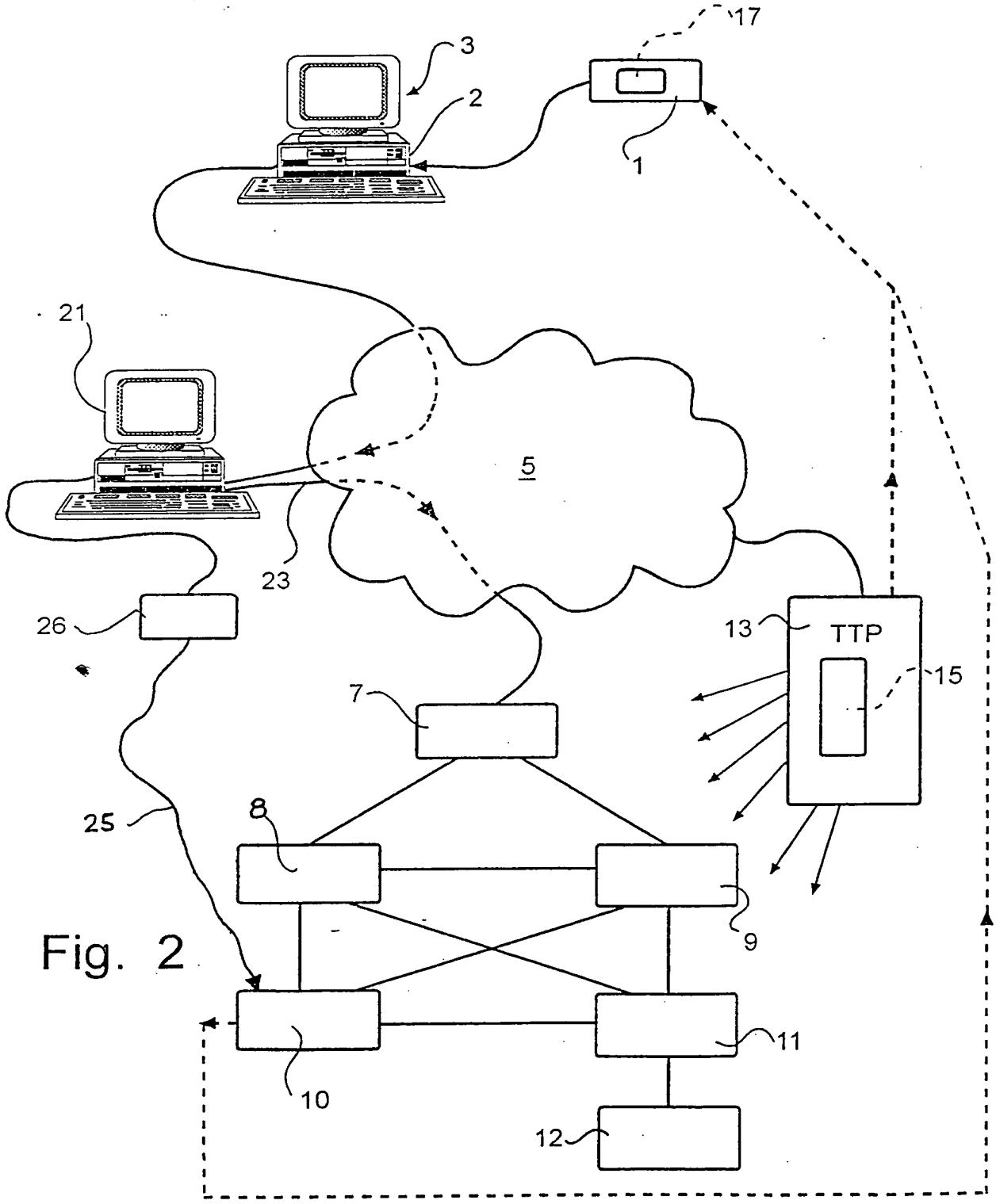


Fig. 2

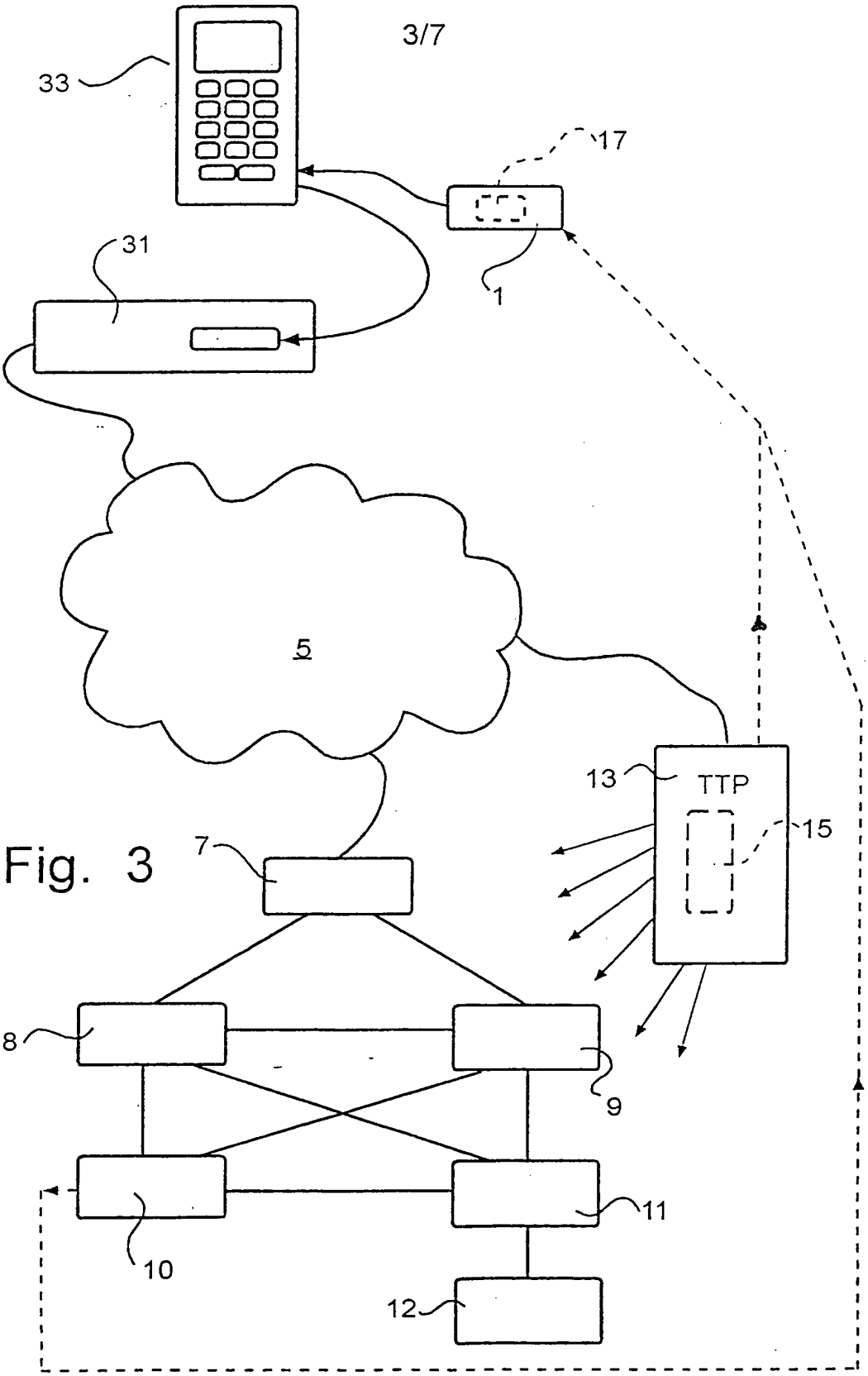


Fig. 3

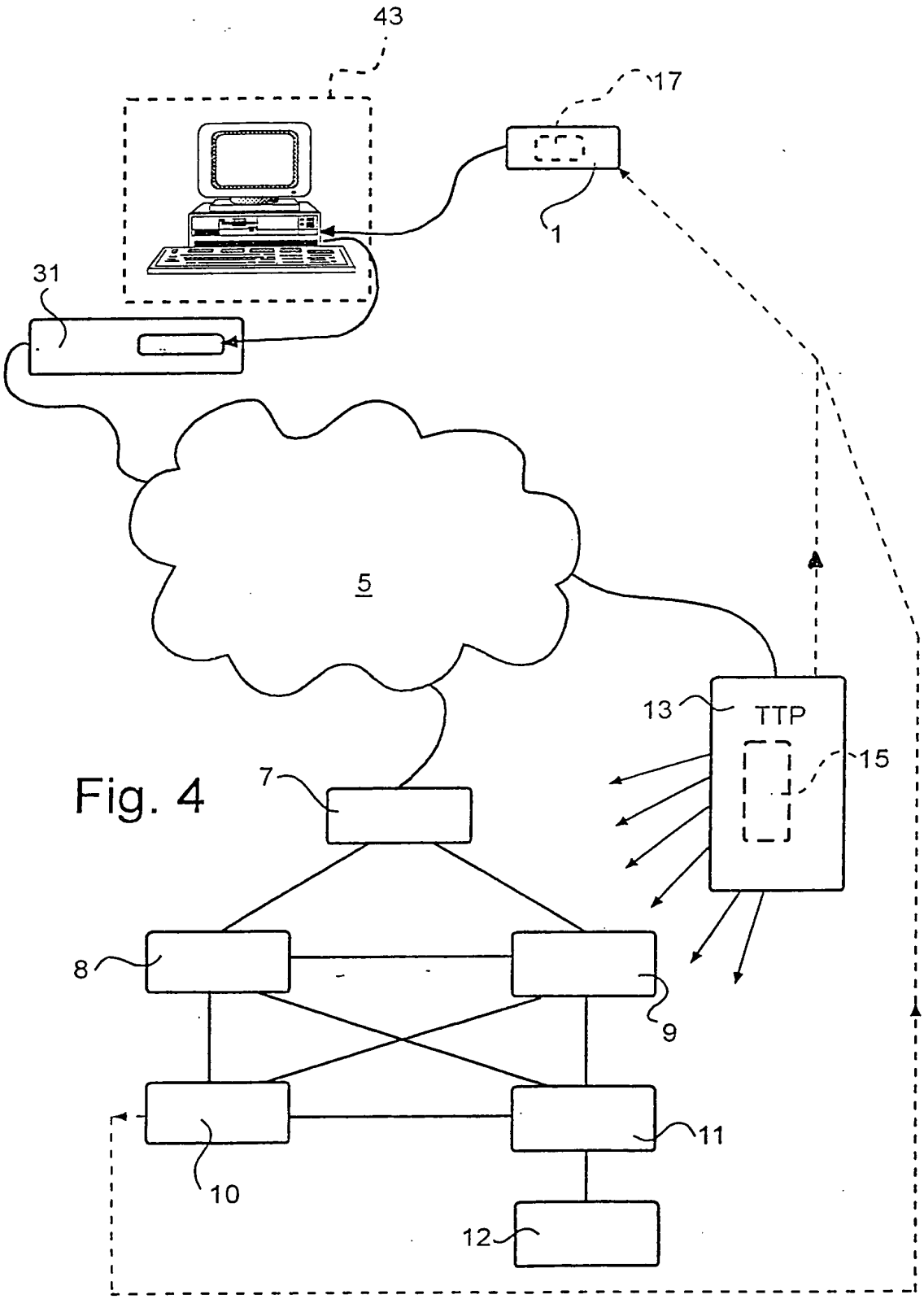


Fig. 4

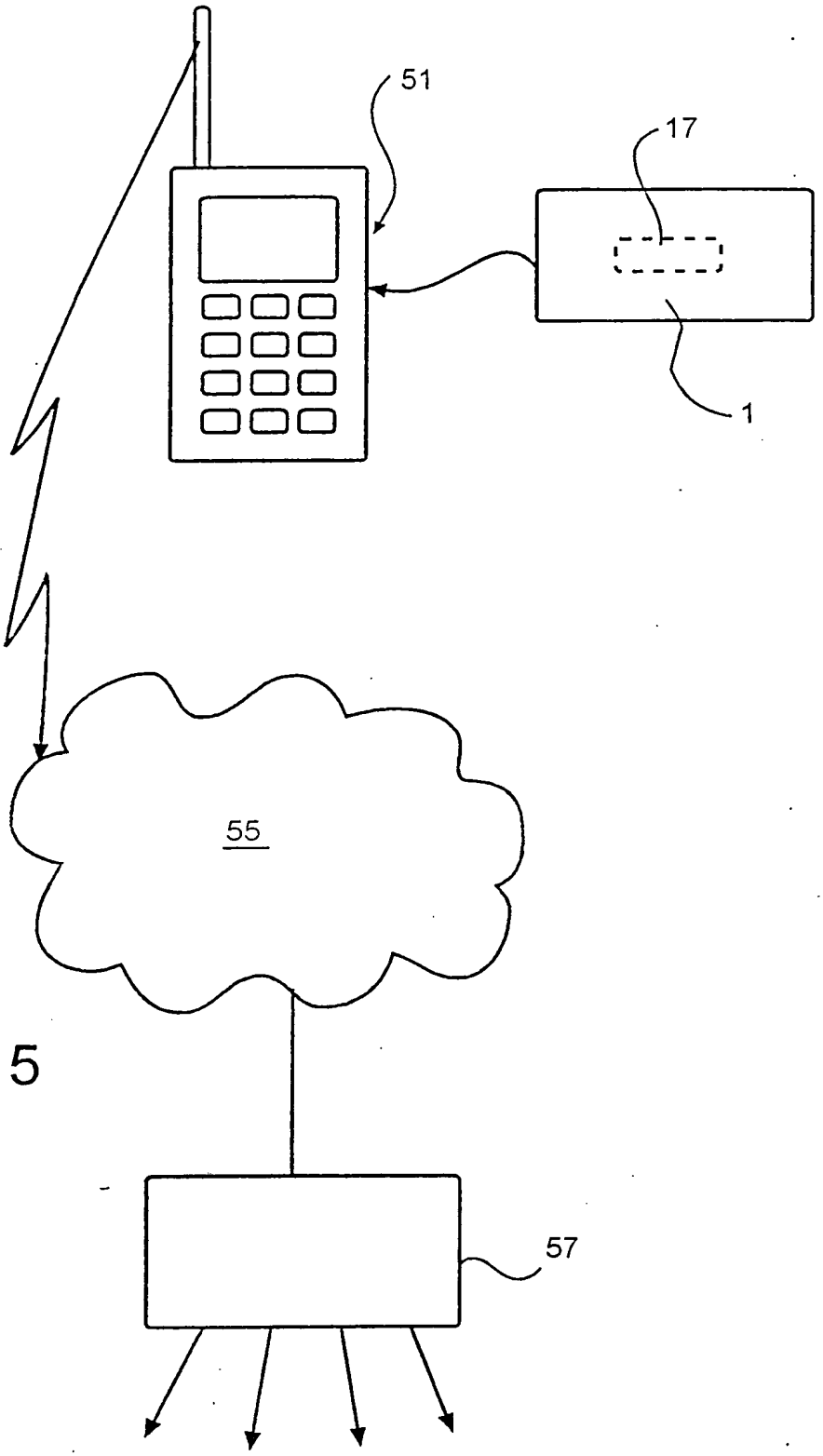


Fig. 5

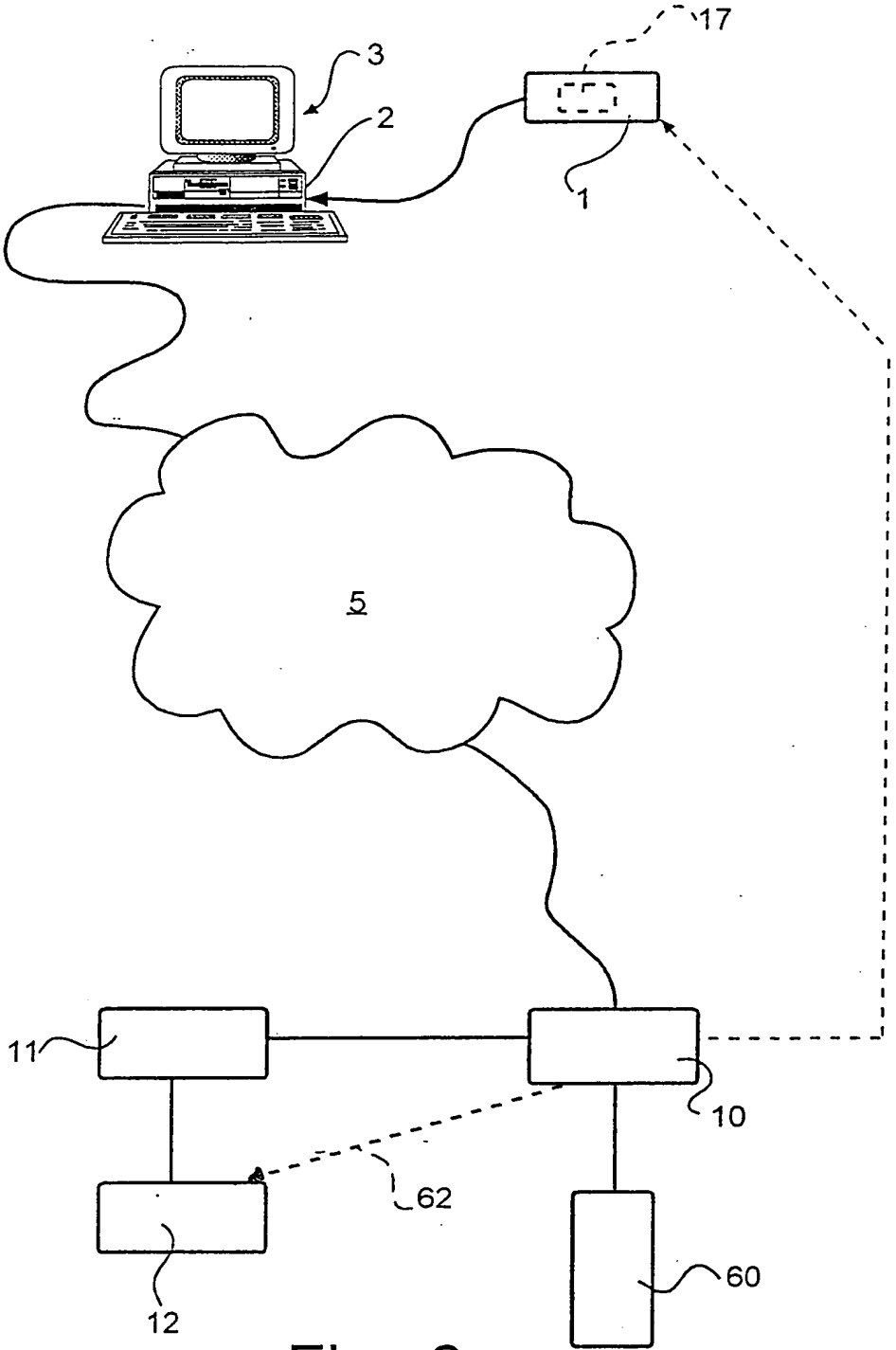


Fig. 6

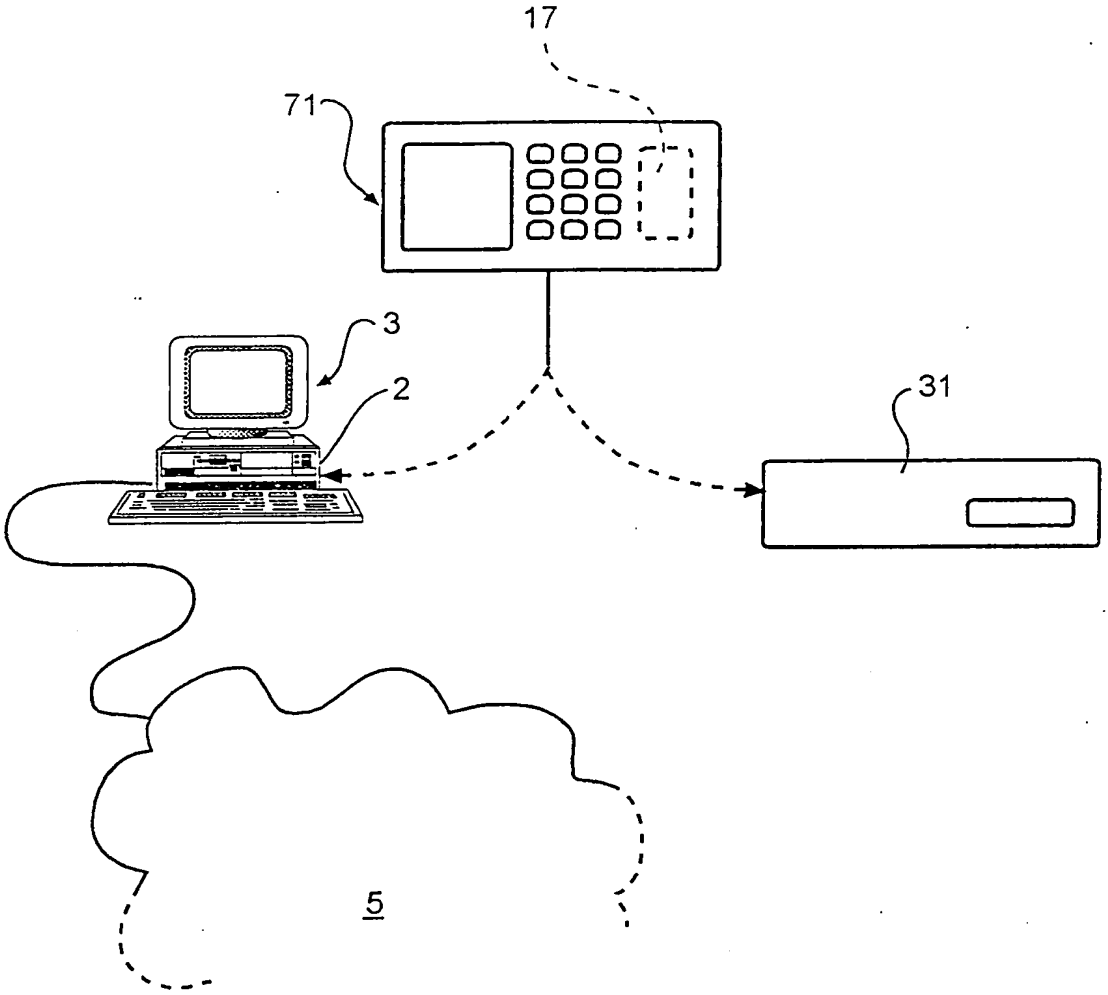


Fig. 7

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G06K 19/00, G07F 19/00, 7/10, H04L 9/32, 9/30

A1

(11) International Publication Number: **WO 98/52151**

(43) International Publication Date: 19 November 1998 (19.11.98)

(21) International Application Number: PCT/SE98/00897

(22) International Filing Date: 14 May 1998 (14.05.98)

(30) Priority Data:
9701814-7 15 May 1997 (15.05.97) SE

(71) Applicant *(for all designated States except US)*: ACCESS SECURITY SWEDEN AB [SE/SE]; Mariebergs Säteri, S-147 92 Grödinge (SE).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: SJÖBLOM, Hans [SE/SE]; Vårgårdsvägen 51, S-133 36 Saltsjöbaden (SE).

(74) Agent: AWAPATENT AB; P.O. Box 45086, S-104 30 Stockholm (SE).

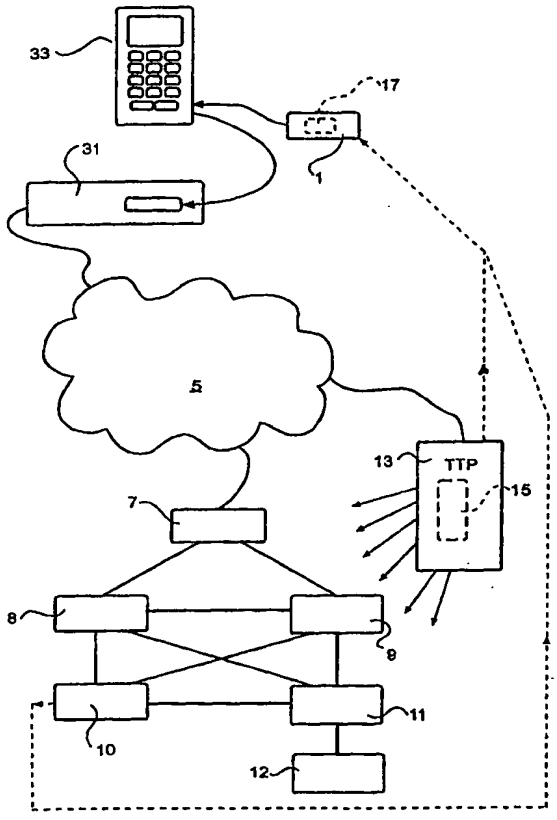
(81) Designated States: AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
In English translation (filed in Swedish).

(54) Title: ELECTRONIC TRANSACTION

(57) Abstract

A method and a device for carrying out electronic transactions. A sender produces, under his own full control, a transaction message in a smart card (1) and provides the message with his digital signature in the card for subsequent output and transmission.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

ELECTRONIC TRANSACTION

Field of the Invention

The present invention relates to electronic transactions, i.e. primarily payments, which are effected electronically. More specifically, the invention concerns electronic transactions effected while employing a user card, such as a cash card, credit card, charge card, or the like, said card being a so-called smart card.

Background Art

In recent years, the interest in electronic transactions has increased significantly, especially concurrently with the impact of the Internet. Security matters have been focused, and different systems and standards have been suggested to guarantee the security in connection with electronic transmission of transaction messages. A matter that has attracted a lot of interest is how to protect, for instance, credit card numbers transmitted via the Internet in connection with Internet shopping. What the systems and standards proposed have in common is that they are based either on the condition that sensitive information that may be misused, for instance a credit card number, is not to be transmitted via the communications network, or on the condition that such sensitive information is to be transmitted in encrypted form. In both alternatives, the relatively complicated administrative routines and system configurations etc. are focused, which, as will be appreciated, results in restrictions and obstacles to a more general use.

Objects of the Invention

A main object of the present invention is to facilitate electronic transactions in a simplified fashion while maintaining full security.

A further object is to facilitate different kinds of electronic transactions within the scope of the same basic concept.

One more object is to facilitate electronic transactions independently of the choice of information transfer channel for the used transaction message.

A still further object is to facilitate electronic transactions which basically do not require transmission of the used transaction message through a reliable information transfer channel.

Summary of the Invention

The above-mentioned objects are achieved by the inventive features that are stated in the accompanying claims.

The invention thus is based on an insight of the advantage of using special transaction messages which, independently and under the user's full control, are created by a user and which are of such nature that they can have been created by the user only, they cannot have been tampered with while being transferred to a receiver or addressee without such tampering being easily recognised (authentication) and can easily be validated after transfer for the purpose of finalising the desired transaction. According to the invention, the sender uses a unique smart card assigned to him, with a private key stored therein (whose public equivalence in an asymmetrical cryptographic system is generally available) in order to provide a transaction message created by the sender with a digital signature which is unique to the sender, whereupon the signed transaction message can be transferred in an arbitrary manner.

Only a lawful user of the smart card can activate this to be signed, thereby satisfying a basic identity requirement. The digital signature further entails a data lock which prevents the message from being tampered with without this being recognised in a subsequent authentication by using the generally available public key, which belongs to the user. The user's independent creating of the transaction message means full control of the contents of the message. The invention thus requires that

sensitive information, such as a card number, in the transmitted transaction message be connected to a digital signature to make the information at issue usable. Without connection to a digital signature, the information thus is basically of no value and consequently cannot be misused for false network transactions, even if the information could be caught by a person not concerned in connection with a transmission of the transaction message. Basically, it is irrelevant how the transmission takes place. This means an approach which is completely opposite to today's striving for the provision of special, reliable, i.e. encrypted, communication systems for transmitting transaction messages via e.g. the Internet.

It is preferred that a transaction message according to the invention contains information on sender, transaction amount and receiver and preferably a variable piece of information, such as a serial number.

According to the invention, the user thus creates what can be said to be a signed "electronic cheque", which can be transmitted in an arbitrary manner and at an arbitrary point of time to an addressee or receiver.

Upon receipt, a transaction message according to the invention can be checked for authenticity by checking the digital signature, whereupon validation and charging or crediting the receiver with the transaction amount at issue can take place in an arbitrary, suitable manner, suitably according to the same principles as apply to the cashing of an ordinary cheque or to clearing in connection with a card purchase.

According to the invention, the transmitted, signed transaction message may contain the required transaction information as plain text, in which case the digital signature can, in a manner known per se, be provided on the basis of a condensate of the message information. This means that the subsequent authentication, validation and crediting on the receiver side will be facilitated since the required information is immediately available, such

as information on sender, which makes it easy to fetch the correct public key for authentication of the digital signature.

If the digital signature is effected on the entire transaction message such that this is transmitted in encrypted form, the transmitted transaction message can be provided with special sender information which makes it possible on the receiver side to fetch the correct public key for authentication and conversion of the transaction message into plain text.

According to the invention, the transaction message may contain sender information of an arbitrary, suitable kind, such as at least one of the following pieces of information: a card number, a cash card number, a charge card number, a credit card number, an account number, an invoice number and an ID number. If the smart card utilised according to the invention is a card connected to an account, such as a credit card, it may be preferred to use the associated card number as sender information. As those skilled in the art realise, it is however possible to use any kind of information, which on the receiver side can easily be connected to a user identity and, consequently, to an associated account which is to be charged.

For the receiver information, basically the same applies. For instance, at least one of the following pieces of information may be involved: a card number, a cash card number, a charge card number, a credit card number, an account number, an invoice number and an ID number. Also in this case, it is sufficient that the information on the receiver side can be unambiguously related to a receiver of payment. It should be noted that transferring a transaction amount to a receiver need not entail the crediting of a receiver account, but it may also imply that e.g. an administrative unit receiving the transaction message, after authentication and validation,

charges a sender account and sends to the receiver what may be considered a check or a postal order.

As described above, an essential feature of the present invention is that the sender, i.e. the user of the smart card, creates and signs the transaction message under his own control, i.e. basically independently of a connection to a communications network and of a computer dialogue with a receiver, although such a dialogue of course may take place in connection with the transmission of a signed transaction message. Consequently the transaction message is created preferably without connection to the communications network or off-line. This means that the sender fully controls which data are input for creating of the transaction message. As will be appreciated, the signing can be carried out only by the sender since in the normal case he is the only one to be able to activate his smart card and to release the signing. Regarding the transmission or handing over of the signed transmission message there are, however, no restrictions, as will be quite easily appreciated. For example, the user or some person assisting him may take the smart card with the signed transaction message present therein to send the message later, to send the message from some other place etc, that is to say there is a great freedom of choice. The signed transaction message could also be transferred to special intermediate materials or a transport medium to be transmitted to a receiver and/or addressee.

According to the invention, it is advantageous that the transaction message is created in the smart card. The transaction message may suitably be created by means of the software inserted in the smart card in advance and sender information preferably inserted in the card in advance, e.g. a card number. Suitably a new serial number is automatically created for each transaction message. The input of the necessary message information in the card may be carried out in different ways, for in-

stance with the aid of the input means arranged on the smart card, the card advantageously consisting of a so-called advanced smart card. Information that is required for the transaction message can also be input with the aid of a protected card terminal, which advantageously may consist of the user's own terminal or computer provided with a card reader. Information that is necessary for the transaction message can also be input by means of a separate card communication unit, the latter preferably later also serving as card activator. Such a unit can advantageously be designed as a small portable unit, which the user may take along and which is utilised by the user when he wants to activate his card and/or input information in the card in surroundings where no protected card terminal is available.

Information which is required for the transaction message can also be input by means of a telecommunications unit controlled by the smart card, especially a mobile telecommunications unit, such as a mobile telephone device. In this context, the unit may also be used to transfer the signed transaction message, for instance by using a so-called SMS-type service.

The man skilled in the art realises that it is also possible to create the actual transaction message outside the smart card by using, for instance, one of the above-mentioned information input means. The created transaction message is then input in the smart card to be signed.

According to a first aspect of the present invention, a method is provided for carrying out electronic transactions, in which a sender of transaction messages is assigned a smart card with an associated unique identity and a private key stored in the card in a protected manner, and in which an associated public key is kept generally available, said method being characterised in that in connection with an electronic transaction under the sender's own control, preferably through his own

input of message information, the sender creates a transaction message, which contains information necessary for the transaction, and, in his smart card, provides the created transaction message with his digital signature while using his own private key for the purpose of subsequent output and transmission of the transaction message.

According to a second aspect of the present invention, a smart card is provided for carrying out electronic transactions, said card comprising means for storing of card identification information, means for protected storing of a private key, means for storing of an asymmetrical algorithm, means for input of transaction information into the card, processor means for creating in the card a transaction message based on input transaction information, such as information on amount and receiver, and optionally information stored in the card, such as information on sender and preferably a serial number, and for providing the transaction message with a digital signature on the basis of said private key and said asymmetrical algorithm, and means for output of the signed transaction message.

According to a third aspect of the present invention, a combination is provided of a smart card and a user-controlled communication unit, which is arranged for communication with the smart card and with which the card is adapted to be combined with a view to producing an electronic transaction message, the card comprising means for protected storing of a private key, means for storing of an asymmetrical algorithm and processor means for providing a created transaction message with a digital signature based on said private key and said algorithm, and said communication unit comprising means for input of transaction information, and means being arranged in the communication unit and/or in the card for producing said transaction message.

A fourth aspect of the present invention involves use of a smart card with a private key stored therein and

asymmetrical cryptographic algorithm for providing in the card, independently of the communications network, an electronic transaction message provided with a digital signature based on the private key.

Additional aspects of distinctive features of the invention will appear from the following detailed description of various embodiments with reference to the accompanying drawings.

Brief Description of the Drawings

Fig. 1 is a schematic illustration of an example of the carrying out of electronic transactions by using an open network, such as the Internet, in accordance with an embodiment of the present invention.

Fig. 2 is a schematic illustration of the same kind as in Fig. 1, exemplifying alternative ways of carrying out electronic transactions according to the invention.

Fig. 3 is a schematic illustration of an example of the carrying out of electronic transactions by using a shop card terminal, according to a different embodiment of the present invention.

Fig. 4 is a schematic illustration of the same kind as in Fig. 3 of another example of the carrying out of electronic transactions by using a shop card terminal, according to the present invention.

Fig. 5 is a schematic illustration of an example of the carrying out of electronic transactions by using a mobile telephone system, according to one more embodiment of the present invention.

Fig. 6 is a schematic illustration of an example of the carrying out of electronic transactions by using an open network for direct contact with a bank, according to another embodiment of the present invention.

Fig. 7 is a schematic illustration of examples showing how an advanced smart card can be used to carry out electronic transactions in accordance with the present invention.

Description of Embodiments

Fig. 1 illustrates schematically a first embodiment of the invention, which can be used for credit card payment via an open network, such as the Internet, between a sender and a receiver included in a network. The sender has access to a smart card 1 and a computer 3 which is provided with a suitable card reader (indicated at 2), and which typically can be a home computer and is connected to the Internet 5. A network server 7 is connected to the network 5 and to various credit card administrators 8 and 9 included in the network. The latter are in conventional manner connected to each other and to various institutions keeping accounts, such as banks 10, 11. In the present example, the sender is supposed to have an account in the bank 10 and a credit card administered by the administrator 8, while the receiver 12 has an account in the bank 11 and a credit card administered by the administrator 9.

A trusted third party (TTP) 13 is network administrator and responsible for the necessary handling of keys. TTP 13 thus assigns to each user his private key which is stored in a protected manner in the user's card 1, and keeps a catalogue 15 available, from which the public key of each user can be collected.

The user's smart card 1, which also has a conventional credit card function, contains in a known manner memory and processor means in the form of one or more integrated circuits (indicated at 17), as well as conventional means for enabling communication between the card and a card reader when the card is placed in the latter.

In addition to the above-mentioned private key, said memory and processor means contain a cryptographic algorithm of an asymmetrical type, which can be a DES algorithm, and software for effecting the signing of a transaction message based on the private key and said cryptographic algorithm. The smart card 1 is activated in an

arbitrary, suitable manner, for instance by means of a PIN input in the card, or biometrically.

When performing a transaction, the card 1 is placed in the card reader 17 of the computer 3 and the card is activated if this has not already been done. A transaction message can now be created in the smart card 1 and/or in the computer 3. If the creation takes place exclusively in the card, which from the viewpoint of security may be preferred, the card also contains software that is suitable for this purpose. In this case, the required information for the transaction message (especially regarding amount and receiver) is input via the keyboard of the computer 3 into the card.

If the actual transaction message is created in the computer, this has been provided with the software required for this purpose, which is suitably supplied to the user in connection with the issuance of the smart card. Also in this case, message information is input via the keyboard.

It is advantageous to use as sender information a card identification, such as the number of the smart card, which is automatically supplied by the card as the transaction message is being created. As receiver information the card number of the receiver can advantageously be input.

After creating the transaction message, it should be provided with a serial number and signed, which, as mentioned above, is effected in the card. If the actual message has been created in the card, it may be desirable, with a view to restricting the software that must be available in the card, to effect the digital signature on the actual message, whereby the message obtains the form of cryptographic text. The signed message which is then transferred must be able to supply information on the sender, thereby making it possible to collect the public key necessary for authentication, as will be described below. Especially if the transaction message is created

in the sender's own protected computer, it may be suitable to generate the digital signature on a condensate of the actual message, which will be available as plain text and also can be transmitted as plain text.

The signed transaction message can now advantageously be given the form of e-mail and then be transmitted via the network 5 to the network server 7.

If the transaction message is available as plain text, the server 7 can, based on the information in the transaction message, directly send the signed message either to the sender's or the receiver's card administrator 8, 9, respectively, for the purposes of authentication and, if authenticity has been established, subsequent validation, charging the sender and crediting the sender with the transaction amount involved, while applying a suitable clearing procedure.

The authentication means that, for instance, the sender's card administrator fetches the sender's public key from a key catalogue of his own or the catalogue 15 of TTP 13 and, by means thereof and of the cryptographic algorithm involved, checks the digital signature of the message.

If the message received by the server is not available as plain text, the server 7 fetches from the catalogue 15 the public key belonging to the sender who can be identified by the received, signed transaction message, e.g. on the basis of special sender information such as a network identity or Internet identity. After conventional decrypting of the message by using the fetched public key, the server 7 has access to the information of the message as plain text and can send the message on for authentication etc, as mentioned above.

One more alternative is to provide the message sent on the network 5 with a stated address of the authorised card administrator, for instance 8, such that the server can directly direct the message to him for continued processing as described above. If the signed message is not

available as plain text, the received message must also in this case provide such information that the correct public key can be fetched for authentication and decryption of the actual message.

Fig. 2 illustrates schematically a second embodiment of the invention, which uses basically the same configuration as in Fig. 1, although the transaction message from the sender is transmitted directly to a receiver's computer 21 via the network 5. The receiver sends the message on, which can be carried out via the network to the server 7, as indicated by the arrow 23, or by some other route as indicated by the arrow 25.

In this embodiment, it may be convenient that the actual message is available as plain text, such that the receiver can see the information therein even if he does not have immediate access to the sender's public key for authentication or decryption of the digital signature. If needed, the signed message can however be encrypted by the sender with a public key belonging to the receiver, in which case the receiver upon receipt decrypts the message by using his own private key and the associated cryptographic algorithm and then forwards the decrypted, but still signed message.

In case of a transport route 25 other than the network 5, it may be advantageous to use intermediate materials, for instance a disk (indicated at 26), which in some suitable and reliable manner, the receiver hands over to his card administrator or bank for continued processing in accordance with that described above. It will be appreciated that the receiver can collect a number of received transaction messages on such intermediate materials before taking steps for the continued processing.

Fig. 3 illustrates schematically an embodiment of the invention which is suited for transactions via a foreign "terminal" 31 and which uses a user-controlled portable unit 33 for creating a transaction message.

The unit 33 consists of a combined activator and information inputting means for the smart card. The unit 33 is in a suitable manner arranged for communication with the card 1, for instance by comprising an integrated card reader, into which the card is inserted. The unit 33 further has a keyboard and a display.

When paying in e.g. a shop, the card is inserted in the unit 33 and activated, for instance, by inputting a PIN code by means of the keyboard of the unit. By means of the keyboard, the necessary payment information is also input, such as amount and receiver. If the transaction message is both created and signed in the actual card, the actual information will be transferred to the card. If the actual message and optionally a condensate thereof are to be created in the unit 33 for the purposes of transferring to and signing in the card 1, the unit is provided with processor means and the software required for this purpose.

The card with the signed transaction message is now removed from the unit 33 and inserted into the shop's reader/terminal 31, from which the message is transmitted for continued processing in the same manner as described above. Accepted authentication and validation may suitably result in a receipt being sent back to the terminal.

It will be appreciated that the terminal 31 could, of course, communicate with the server 7 in some other manner than via the network 5, for instance via a protected connection.

Fig. 4 illustrates a variant of the embodiment shown in Fig. 3. The unit 33 in Fig. 3 is replaced by a protected, preferably off-line computer or terminal 43, which can be arranged in, for instance, a shop and permits off-line, secure creation of a transaction message in a way similar to that described in connection with Fig. 3, for the purposes of input in a shop card terminal 31.

Fig. 5 illustrates an embodiment of the present invention which involves the use of a mobile telephone device 51 and an associated mobile telephone network 55. The mobile telephone device comprises, in addition to a mobile telephone function, also such an activating and input function as described in connection with the unit 33 in Fig. 3. The mobile telephone function is preferably also controlled by the smart card.

With the aid of the telephone function, the signed transaction message is transmitted to a unit or central unit 57, which effects continued processing of the transaction message, for instance, in accordance with that described in connection with the preceding Figures.

The transmission of the transaction message can advantageously take place while using a so-called SMS service or the like of the mobile telephone network.

The unit 57 could also be a special central unit, which after authentication etc. effects payments based on the received transaction messages.

Fig. 6 illustrates an embodiment of the present invention which advantageously can be used to effect payment orders. At a sender's, i.e. payer's place, signed transaction messages are created as described, in this case exemplified with the same method as in Fig. 1. The transaction message is transmitted to the sender's bank 10 keeping the account, which in a catalogue 60 has access to the sender's public key. It will be appreciated that the bank could be card issuer and key administrator and that the sender information in the transaction message can suitably consist of the sender's bank account number.

Upon receipt of a transaction message and authentication thereof, the sender's bank 10 provides for, by a clearing procedure, the payee, who is identified in the transaction message suitably by the associated bank account number, being credited with the amount at issue,

i.e. the receiver's account in the receiver's bank 11 being credited with the amount at issue.

Another alternative possibility is that the sender's bank 10 sends a delivery order directly to the receiver 12 based on, for instance, receiver information in the transaction message. This alternative is indicated by means of the dashed line 62 in Fig. 6.

In the embodiment according to Fig. 6 it may be convenient to encrypt the transmitted, signed transaction message, thereby increasing the security. The sender then uses the public key of the bank 10 and preferably the same cryptographic algorithm as is used for signing. As will be appreciated, the bank 10 can immediately carry out decryption by using its private key.

If the bank 10 is administrator of the sender's pair of keys, i.e. has both the public key and the private key belonging to the sender, the sender can alternatively carry out the encryption of the signed message with the aid of his public key. The bank 10 can then decrypt the transmitted message by using the sender's private key, which is collected from a catalogue, before authentication is carried out by using the sender's public key.

Finally, Fig. 7 illustrates schematically the use of a so-called advanced smart cart in connection with the invention. The advanced smart card 71 also has a keyboard and a display, which allows that a signed transaction message can be created in the card completely without external aids. Subsequently the card can be inserted into e.g. a computer or a terminal for the purposes of forwarding the message and continued processing in accordance with that described above.

Although the invention has been illustrated by a number of embodiments, the invention is of course not restricted thereto, and changes and modifications are feasible within the scope of the appended claims. Thus, individual features from the various embodiments may be brought together in new combinations within the scope of the inventive idea.

CLAIMS

1. A method for performing electronic transactions, in which a sender of transaction messages is assigned a smart card with an associated unique identity and a private key stored in the card in a protected manner, and in which an associated public key is kept generally available, c h a r a c t e r i s e d in that in connection with an electronic transaction under the sender's own control, preferably through his own input of message information, the sender creates a transaction message, which contains information necessary for the transaction, and, in his smart card, provides the created transaction message with his digital signature while using his own private key for subsequent output and transmission of the transaction message.

2. A method as claimed in claim 1, c h a r a c t e r i s e d in that the transaction message contains information on sender, receiver, amount and preferably a transaction serial number.

3. A method as claimed in claim 1 or 2, c h a r a c t e r i s e d in that the transaction message is created off-line, i.e. not connected to the communications network that is used for the subsequent transmission of the transaction message.

4. A method as claimed in claim 3, c h a r a c t e r i s e d in that the transaction message is created off-line.

5. A method as claimed in any one of the preceding claims, c h a r a c t e r i s e d in that the transaction message is created in the smart card.

6. A method as claimed in claim 5, c h a r a c t e r i s e d in that the transaction message is created with the aid of software inserted in the smart card in advance and preferably also sender information inserted in the card in advance.

7. A method as claimed in claim 5 or 6, c h a r - a c t e r i s e d in that information required for the transaction message is input with the aid of input means arranged on the smart card, the card preferably being a so-called advanced smart card.

8. A method as claimed in any one of claims 1-6, c h a r a c t e r i s e d in that information necessary for the transaction message is input with the aid of a protected card terminal.

9. A method as claimed in any one of claims 1-6, c h a r a c t e r i s e d in that information necessary for the transaction message is input with the aid of a separate card communication unit, the latter preferably also being a card activator.

10. A method as claimed in any one of claims 1-6, c h a r a c t e r i s e d in that information necessary for the transaction message is input with the aid of a telecommunications unit controlled by the smart card, especially a mobile telecommunications unit such as a mobile phone.

11. A method as claimed in any one of the preceding claims, c h a r a c t e r i s e d in that the transaction message contains sender information in the form of at least one of the following pieces of information: a card number, a cash card number, a charge card number, a credit card number, an account number, an invoice number and an ID number.

12. A method as claimed in any one of the preceding claims, c h a r a c t e r i s e d in that the transaction message contains receiver information in the form of at least one of the following pieces of information: a card number, a cash card number, a charge card number, a credit card number, an account number, an invoice number and an ID number.

13. A method as claimed in any one of the preceding claims, c h a r a c t e r i s e d in that the signed transaction message is sent to a card or account admini-

strator regarding the sender or receiver, that the digital signature of the transaction message is authenticated by using the public key, which is assigned to the one who is identified as sender by the transmitted transaction message, and that in case of authenticity, the receiver is credited with the transaction amount by a clearing process.

14. A method as claimed in claim 13, c h a r a c t e r i s e d in that the signed transaction message is first sent to the receiver, who optionally after his own checking of the digital signature of the message forwards the signed transaction message to said card or account administrator.

15 A method as claimed in any one of claims 1-12, c h a r a c t e r i s e d in that the signed transaction message is encrypted by using a public key belonging to the addressee, to whom the transaction message is sent, that the encrypted, signed transaction message is sent to the addressee, that the addressee by using his private key decrypts the signed transaction message, that the digital signature of the transaction message is authenticated by using the public key which is assigned to the one who is identified as sender by the transmitted transaction message, and that the receiver, in case of authenticity, is credited with the transaction amount by a clearing process.

16. A method as claimed in claim 15, c h a r a c t e r i s e d in that the addressee is the receiver, that the receiver, after decryption, sends the signed transaction message to a card or account administrator, whereupon said authentication takes place.

17. A method as claimed in any one of claims 1-12, c h a r a c t e r i s e d in that the signed transaction message is encrypted by using the sender's public key and is provided with sender information and is then sent to a card or account administrator, who has the sender's private key and who preferably has issued the user's smart

card, that said administrator decrypts the received encrypted message by using said private key, that authentication of the digital signature of the decrypted transaction message takes place by using the public key, which is assigned to the one who is identified as sender by the transmitted transaction message, and that the receiver, in case of authenticity, is credited with the transaction amount by a clearing process.

18. A method as claimed in any one of claims 1-14, c h a r a c t e r i s e d in that the signed transaction message is sent non-encrypted, especially via a public communications network, such as the Internet or a telecommunications network.

19. A method as claimed in any one of the preceding claims, c h a r a c t e r i s e d in that the signed transaction message is sent by e-mail.

20. A method as claimed in any one of claims 1-18, c h a r a c t e r i s e d in that the signed transaction message is sent via a mobile telephone network, especially by using a so-called SMS service.

21. A smart card for carrying out electronic transactions, comprising means for storing card identification information, means for protected storing of a private key, means for storing an asymmetrical algorithm, means for input of transaction information into the card, processor means for creating in the card a transaction message based on input transaction information, such as information on amount and receiver, and optionally information stored in the card, such as information on sender and preferably a serial number, and for providing the transaction message with a digital signature on the basis of said private key and said asymmetrical algorithm, and means for output of the signed transaction message.

22. A card as claimed in claim 21, c h a r a c t e r i s e d in that it is of a so-called advanced type.

23. A combination of a smart card and a user-controlled communication unit, which is arranged for commu-

nication with the smart card and with which the card is adapted to be combined with a view to producing an electronic transaction message, the card comprising means for protected storing of a private key, means for storing an asymmetrical algorithm and processor means for providing a created transaction message with a digital signature based on said private key and said algorithm, and said communication unit comprising means for input of transaction information, and means being arranged in the communication unit and/or in the card for creating said transaction message.

24. A combination as claimed in claim 23, c h a r a c t e r i s e d in that the communication unit is a mobile telecommunication device.

25. A combination as claimed in claim 23, c h a r a c t e r i s e d in that the communication unit is a combined card activator and information inputter/processor.

26. Use of a smart card with a private key stored therein for providing, independently of the communications network, an electronic transaction message provided with a digital signature based on the private key.

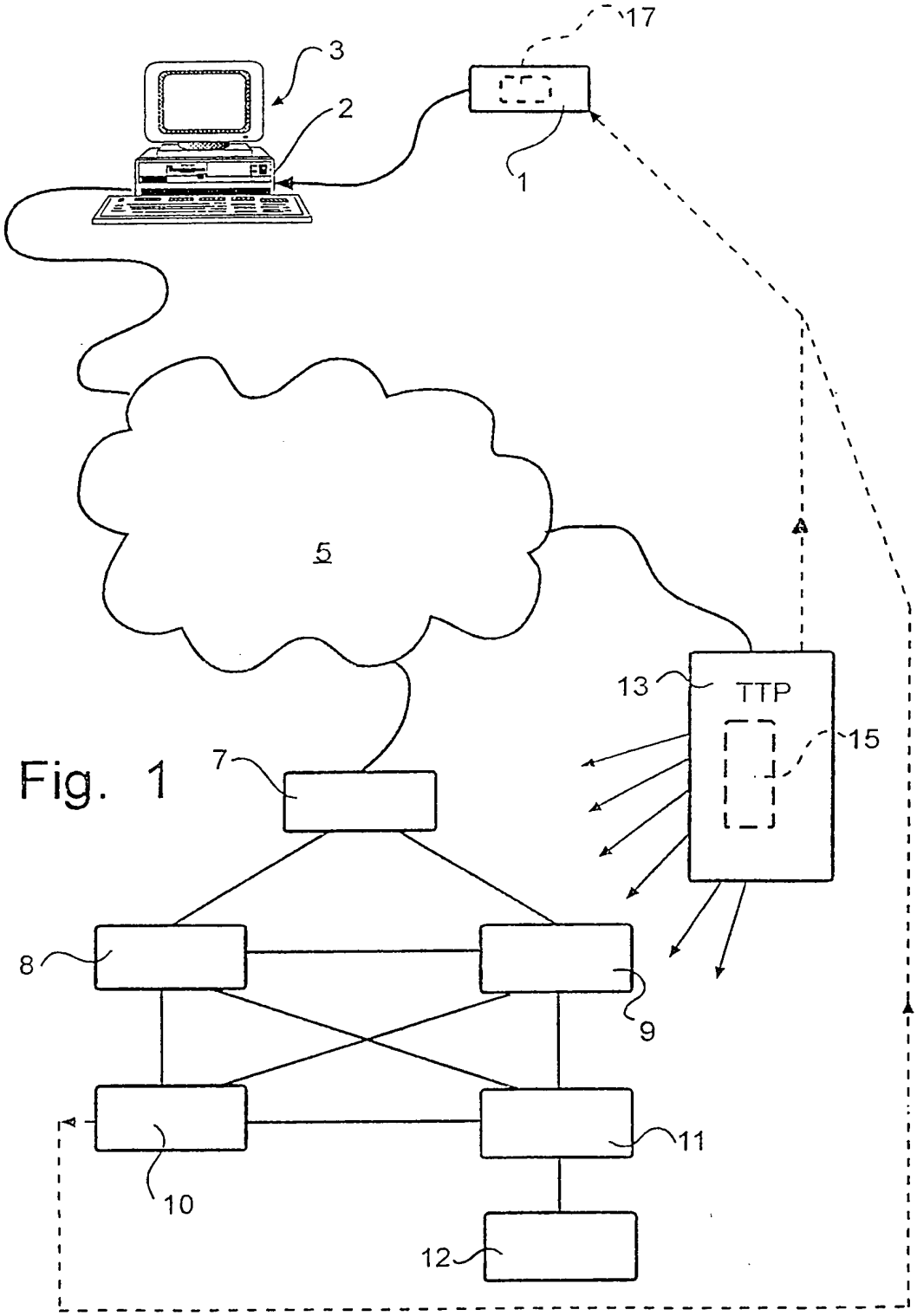


Fig. 1

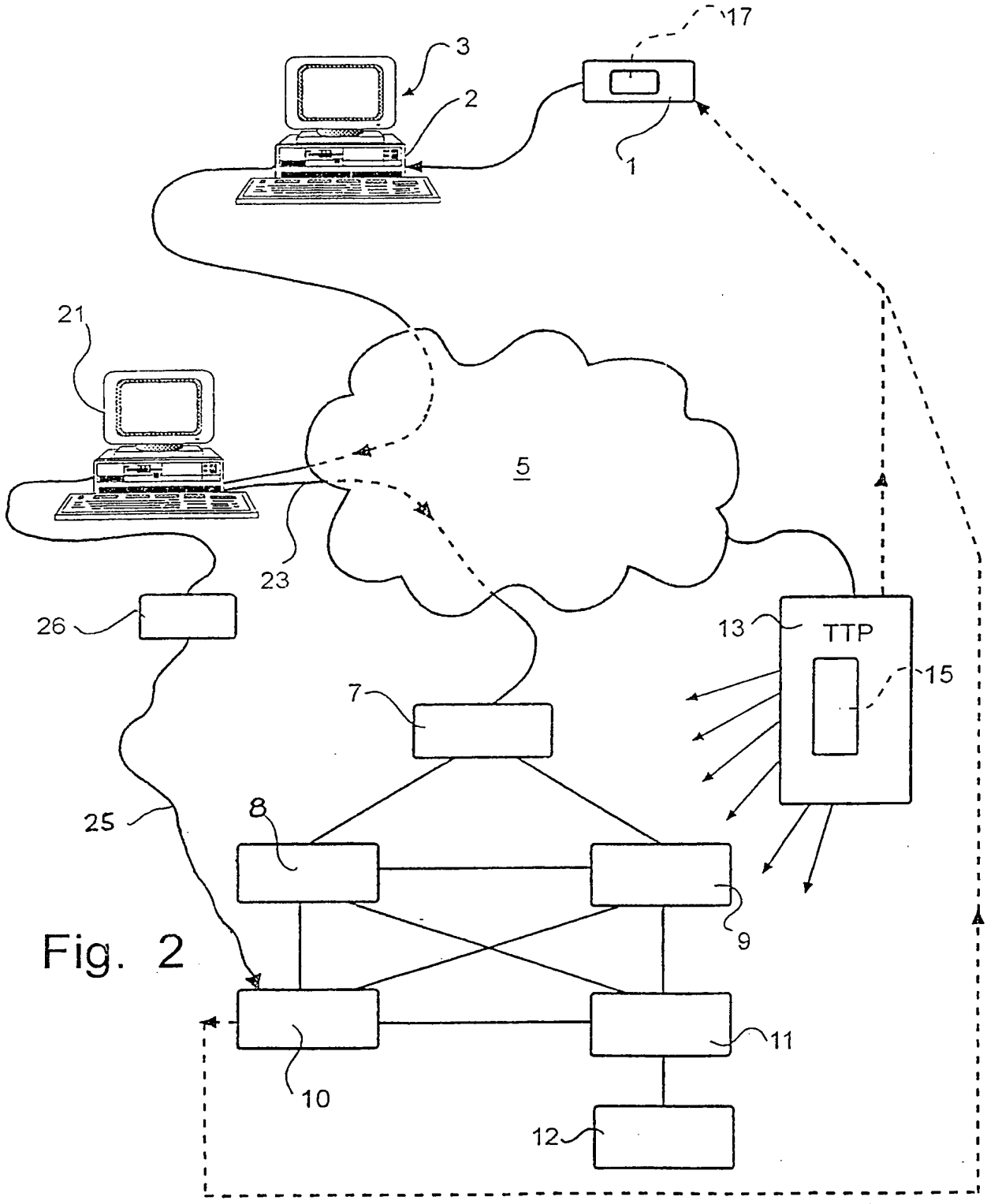


Fig. 2

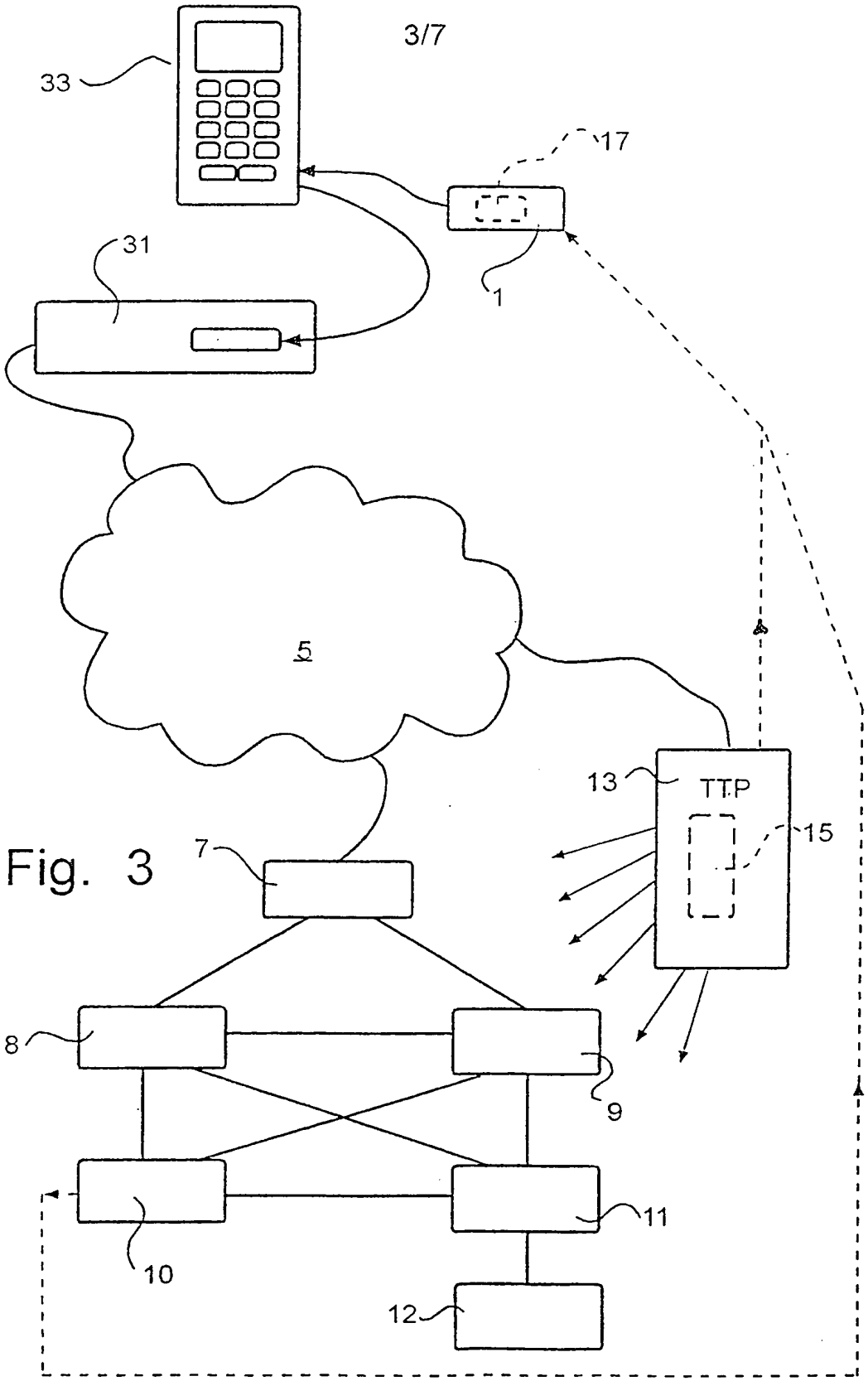


Fig. 3

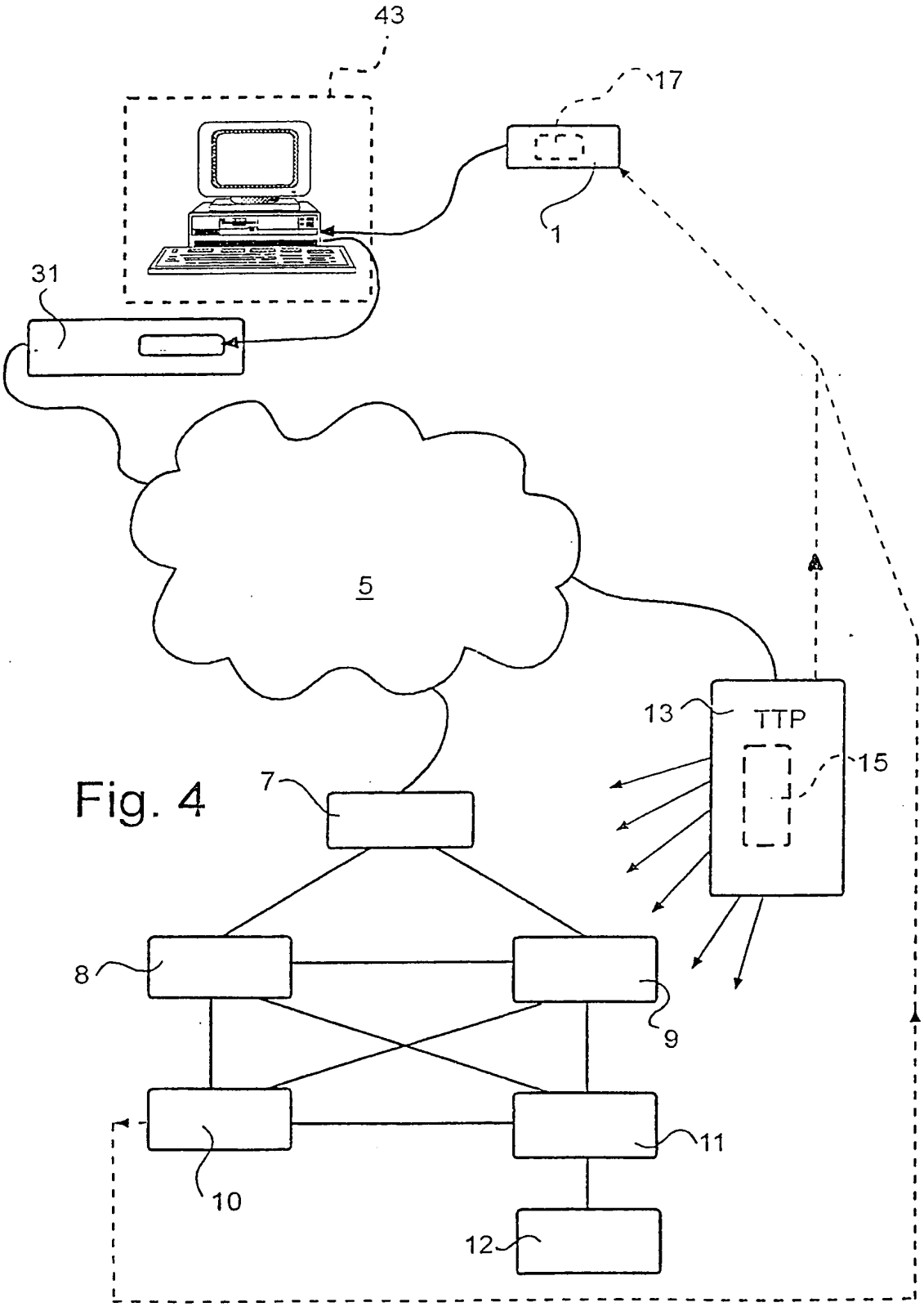


Fig. 4

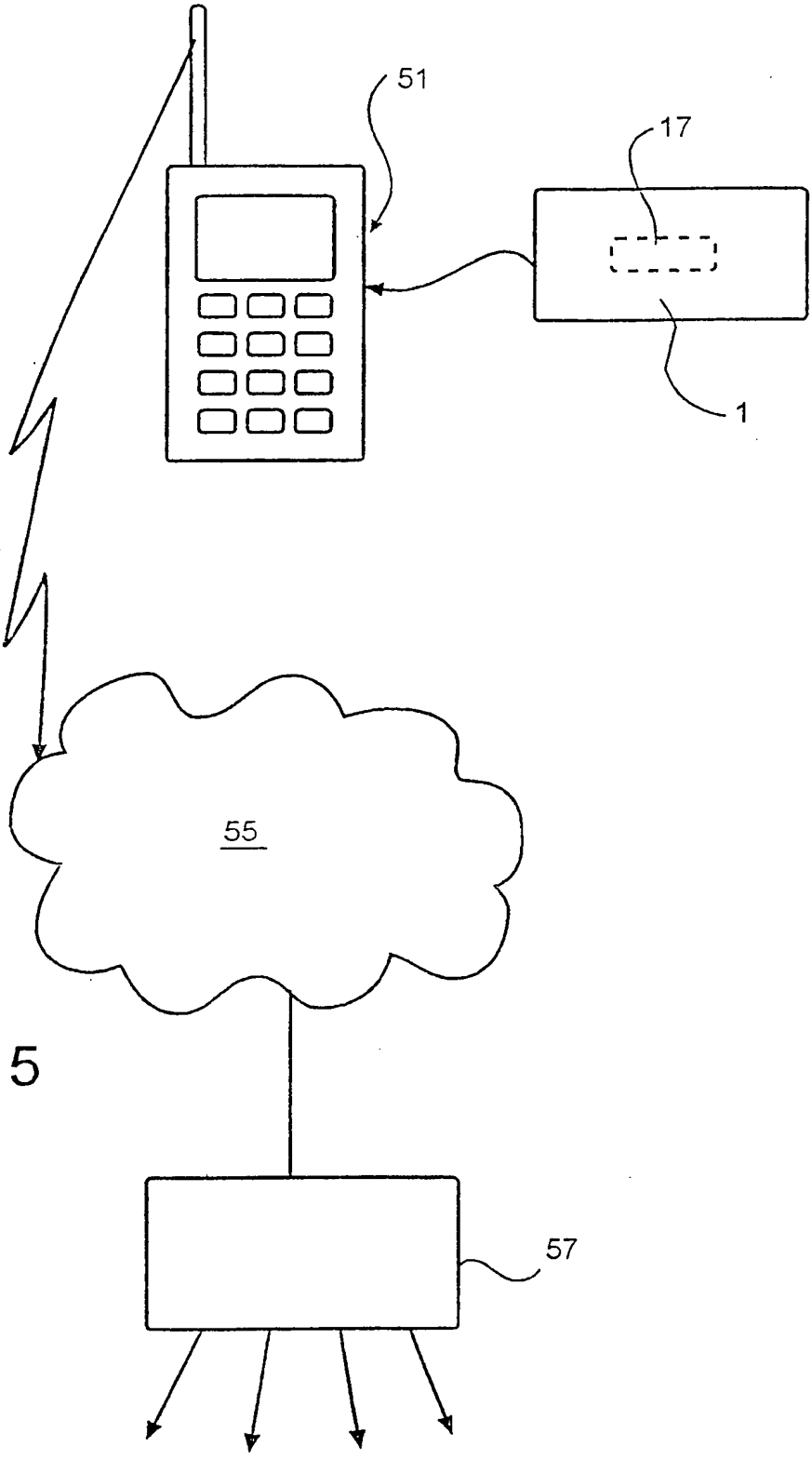


Fig. 5

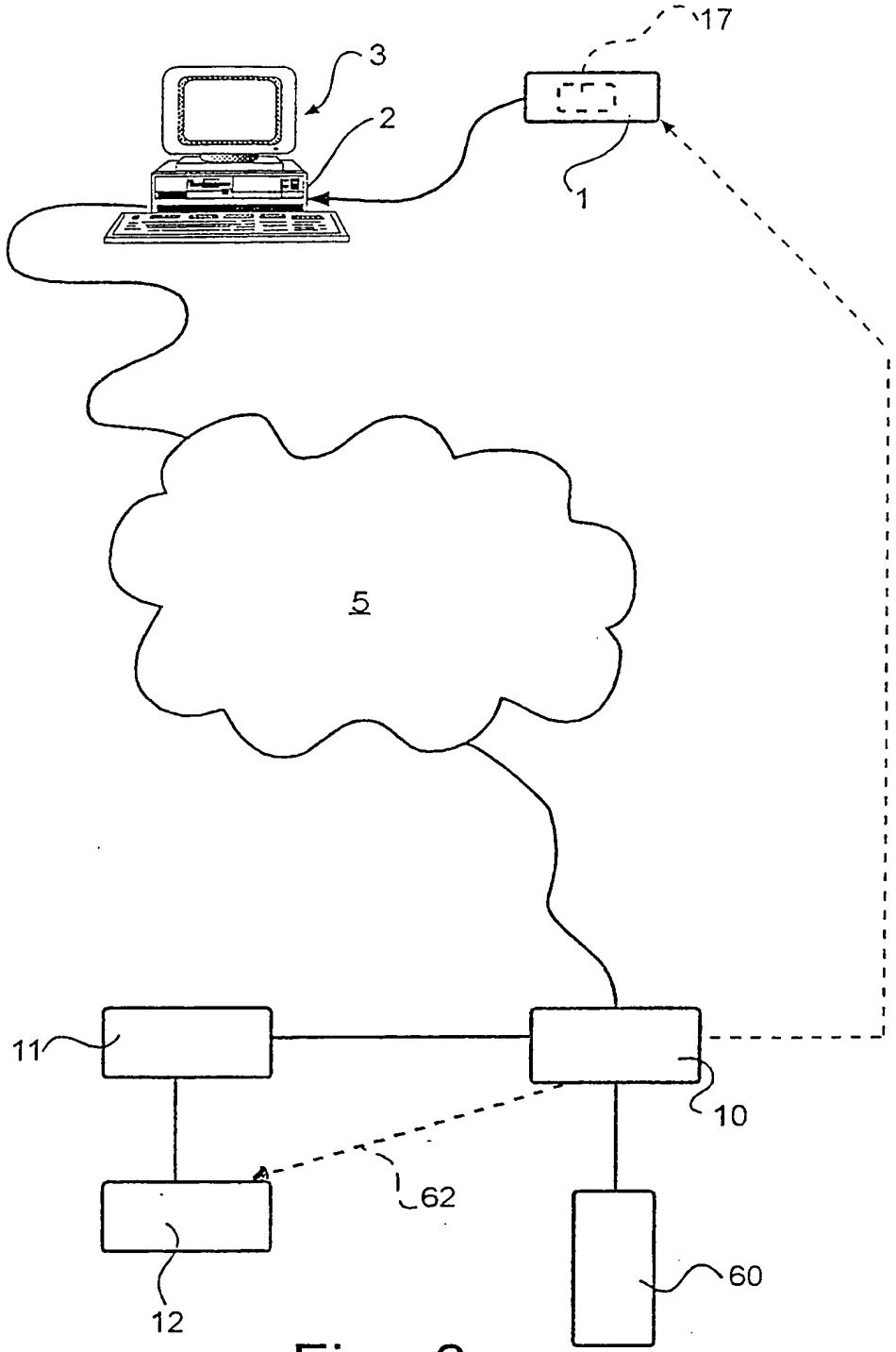


Fig. 6

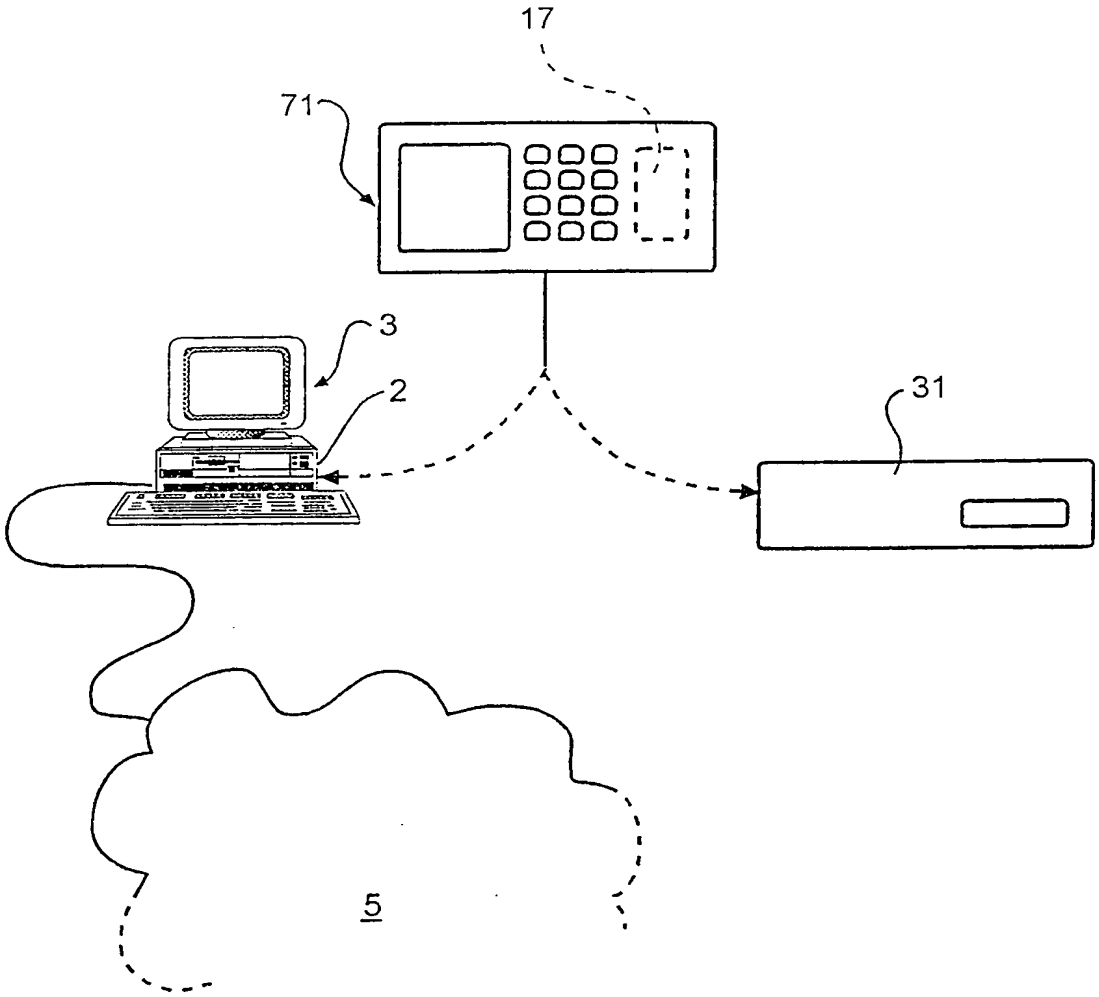


Fig. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 98/00897

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: G06K 19/00, G07F 19/00, G07F 7/10, H04L 9/32, H04L 9/30
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: G06K, G07F, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0214609 A2 (HITACHI, LTD.), 18 March 1987 (18.03.87), column 26, step 5010, column 28, step 5090, column 30, line 38 - line 46	1-4,10-20
Y		5-9
	--	
X	US 4926480 A (D. CHAUM), 15 May 1990 (15.05.90), column 7, line 1 - line 13, figure 1	21-26
Y		5-7
	--	
Y	US 5130519 A (G. BUSH ET AL), 14 July 1992 (14.07.92), column 5, line 49 - line 59, figure 2	8-9
A		21-26
	--	

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 Sept 1998	03 -09- 1998
Name and mailing address of the ISA Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Henrik Bodin Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 98/00897

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0166541 A2 (KABUSHIKI KAISHA TOSHIBA), 2 January 1986 (02.01.86), abstract --	1,21
A	EP 0385400 A2 (ATALLA CORPORATION), 5 Sept 1990 (05.09.90), abstract --	1
A	US 5502765 A (G. ISHIGURO ET AL), 26 March 1996 (26.03.96), abstract --	1,21-26
A	US 4849613 A (R.H. EISELE), 18 July 1989 (18.07.89), abstract --	1-26
P,A	US 5721781 A (V. DEO ET AL), 24 February 1998 (24.02.98), abstract --	1-26
E,A	WO 9825220 A1 (INSTITUTE OF SYSTEMS SCIENCE), 11 June 1998 (11.06.98), abstract -- --------	1-26

INTERNATIONAL SEARCH REPORT

Information on patent family members

27/07/98

International application No.
PCT/SE 98/00897

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0214609 A2	18/03/87	DE 3687934 A	15/04/93
		JP 62056043 A	11/03/87
		US 4885777 A	05/12/89
		US 5018196 A	21/05/91
US 4926480 A	15/05/90	AT 156639 T	15/08/97
		AU 3771489 A	12/12/89
		DE 68928240 D	00/00/00
		EP 0418328 A,B	27/03/91
		EP 0773647 A	14/05/97
		JP 3505032 T	31/10/91
		WO 8911762 A	30/11/89
		DE 3485804 A	13/08/92
		EP 0139313 A,B	02/05/85
		SE 0139313 T3	
		US 4759063 A	19/07/88
US 5130519 A	14/07/92	US 5265162 A	23/11/93
EP 0166541 A2	02/01/86	JP 61009052 A	16/01/86
		US 4823388 A	18/04/89
EP 0385400 A2	05/09/90	SE 0385400 T3	
		AU 615832 B	10/10/91
		AU 5052790 A	06/09/90
		CA 2010345 A	01/09/90
		DE 69019037 D,T	12/10/95
		JP 3067355 A	22/03/91
		US 4965568 A	23/10/90
US 5502765 A	26/03/96	EP 0588339 A	23/03/94
		JP 6103425 A	15/04/94
		US 5396558 A	07/03/95
		US 5446796 A	29/08/95
		JP 6103426 A	15/04/94
		JP 6162289 A	10/06/94
		JP 6162287 A	10/06/94
		JP 6161354 A	07/06/94
US 4849613 A	18/07/89	AU 573872 B	23/06/88
		AU 4538085 A	29/01/87
		DE 3417766 A	14/11/85
		DK 208185 A	13/11/85
		EP 0172314 A	26/02/86
		JP 61033574 A	17/02/86
US 5721781 A	24/02/98	NONE	
WO 9825220 A1	11/06/98	NONE	